УДК 001.6+004

И.А. Громыко

Харьковский национальный университет им. В.Н. Каразина, Харьков

ЗАЩИТА ИНФОРМАЦИИ И ЗАДАЧА КОШИ

В данной статье приведены рекомендации для систем защиты информации на основании математической процедуры приведения сложной граничной задачи к задаче Коши.

Ключевые слова: *защита информации, задача Коши.*

Введение

Постановка проблемы. Исследование проблематики, касающейся защиты информации, в категориях предметной области приводит к выводу о целесообразности последовательного рассмотрения дискретных носителей, механизмы переноса которых, как правило, различны. Иначе говоря, вместо «чёрного ящика», для которого известны вход, выход и внутренняя структура гораздо более эффективным представляется изучение «перемещения» информации вдоль, по цепочке носителей (рис. 1) [1].

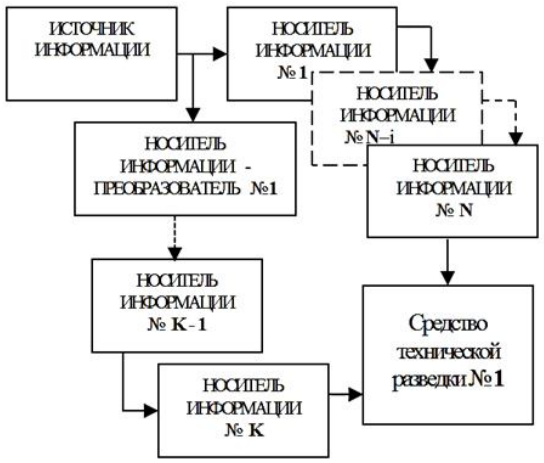

Рис. 1. Реальная структурная схема технического канала утечки информации

Здесь видится аналогия с методами, которые широко используются для численной реализации граничных задач.

В подтверждение данного соображения приведём выдержку:

«Исходная идея этой книги состоит в том, что вычислительные машины по самой своей природе являются наиболее эффективным средством для решения дифференциальных уравнений, начальные условия которых заданы в одной точке, т.е. так называемых «задач Коши».

С другой стороны, многие задачи, возникающие в математической физике, технике, биологии, экономике и исследовании операций, по своей природе являются граничными, поскольку необходимые для однозначного определения условия задаются в двух или более точках.

Но надо сказать, что цифровые вычислительные машины, вообще говоря, не слишком хорошо приспособлены для численного решения таких задач. Основная мысль, развиваемая в этой книге, состоит в следующем: формулируя математически какую-либо задачу, следует учитывать имеющиеся вычислительные средства, ибо часто существуют иные эквивалентные формулировки задачи, которые в вычислительном отношении выгодно отличаются от начальной» [2, с. 10].

Конечно, в данном случае авторы подразумевают исходную формулировку, поскольку «начальной» зачастую называют собственно задачу Коши.

И далее, в том же контексте:

«Теория инвариантного погружения заставляет переосмыслить наше понимание того, как следует ставить математические задачи. Формулировка задачи, удовлетворительная для аналитического исследования, может оказаться неудачной с вычислительной точки зрения и наоборот» [2, с. 15].

Возникает вопрос: нельзя ли предположить, что на самом деле, имеет место большее, чем аналогия (о ней упоминалось выше)?

Целью статьи является выработка рекомендаций для систем защиты информации на основании математической процедуры сведения сложной граничной задачи к задаче Коши.

Основная часть

Изучение исследований и публикаций. Разработка рекомендаций. На абстрактном уровне, мы вполне можем предположить, что у процессов распространения информации, в пределах её носителей, есть свои дифференциальные уравнения. Однако чем привлекательна задача Коши?

Ответ простой: предельно конструктивны как теория этого класса задач, так и алгоритмы их численной реализации. К этому следует добавить ещё и широкую область практических приложений.

В математической интерпретации данные утверждения характеризует выдержка:

«Рассмотрим теперь следующую задачу Коши:

$$d_t z = h(z, t),\ z(0) = c,$$

где **z**, **h** и **c** суть n – мерные векторы.

Пусть **R** – область в $\mathbf{R}^n$, заданная формулой

$$\|z - c\| \le k_1,$$

и пусть $k_2 = \max \|h(z, t)\|$ по всем $z \in R$.

Имеет место следующая теорема существования и единственности:

*Если h(z,t) – непрерывная функция от Z в R и если для любых двух векторов **x** и **y** из **R** существует постоянная k_3, которая:*

*– не зависит от **x** и **y**, и такая, что*

$\|h(x, t) - h(y, t)\| \le k_3 \|x - y\|$ (1), *то задача обладает единственным решением при всех* $0 \le t \le k_1 / k_2$ » [2, с. 31].

Здесь (1) – условие Липшица.

В скалярном случае:

$d_t u = h(u, t),\ u(0) = c$

можно использовать аппроксимацию

$u(t + \Delta) \cong u(t) + h(u, t)\Delta,\ u(0) = c$ (2), (она является простейшей), где Δ – малый параметр. Вычисление $u(\Delta)$, $u(2\Delta)$ и т.д. – «как раз та задача, для решения которой ЭВМ идеально приспособлена» [2, с. 31, 32].

Пусть не покажется излишне пространной математическая символика, поскольку алгоритм (2), а также, в первую очередь, следующая выдержка и комментарии к ней, выводят нас на весьма нетривиальные соображения в отношении предмета настоящего исследования.

«Следует отметить одно важное обстоятельство, а именно, что двухточечные граничные условия принципиально отличаются от условий, заданных в одной точке, в отношении существования и единственности решения.

Легко построить двухточечную граничную задачу, которая в зависимости от длины интервала имеет одно решение, бесконечно много решений или не имеет решений вообще.

Это резко отличается от ситуации, устанавливаемой теоремой существования и единственности для задачи Коши» [2, с. 43].

Заметим, что осложнения, возникающие при численной реализации двухточечных граничных задач методом конечных разностей на этапе решения систем линейных алгебраических уравнений, детально проанализированы в [3, п. 3].

В качестве иллюстрации сказанного, приведём весьма колоритный пример [4, с. 57, 58], привязав его к термину «информация». Пусть два информационных продукта ценой $C_1 = 4{,}11$ и $c_2 = 9{,}7$ комплектуются также из двух компонентов в пропорции:

$$\left.\begin{aligned} 4{,}1x_1 + 2{,}8x_2 &= 4{,}11; \\ 9{,}7x_1 + 6{,}6x_2 &= 9{,}70, \end{aligned}\right\} \quad (3)$$

где $\mathbf{x_1}$, $\mathbf{x_2}$ – цены за единицу каждого компонента.

Решением системы линейных алгебраических уравнений (3) являются значения $\mathbf{x_1} = 0{,}34$; $\mathbf{x_2} = 0{,}97$.

Однако если цена первого продукта очень ненамного уменьшилась, до величины $\mathbf{c_1} = 4{,}1$, тогда как остальные параметры системы (3) не изменились, её решение становится совершенно абсурдным: $\mathbf{x_1} = 1$; $\mathbf{x_2} = 0$.

Причина в том, что число обусловленности в данном случае составляет **2249,4**. Это число является мерой увеличения погрешности решения вследствие малой вариации параметров (3).

Итак, наши выводы, сугубо практической направленности, что следует подчеркнуть, состоят в следующем:

1. Анализ информационной безопасности и реализация соответствующих мероприятий должны производиться строго в порядке последовательного расположения носителей.

2. Решающее значение для защиты информации имеет эффективность мероприятий, которые предусмотрены в начальные моменты её поступлений на каждый из носителей, включая, естественно, **t = 0** (2). Здесь для наглядности, будет уместным показ обобщённого примера санкционированного распространения ИСОД с выполнением обязательных условий (подкреплённым мероприятиями), в соответствии с требованиями законов Украины и специальных инструкций. Основная часть условий приведена на рис. 2, получившем условное название «пирамида секретности» или «пирамида конфиденциальности».

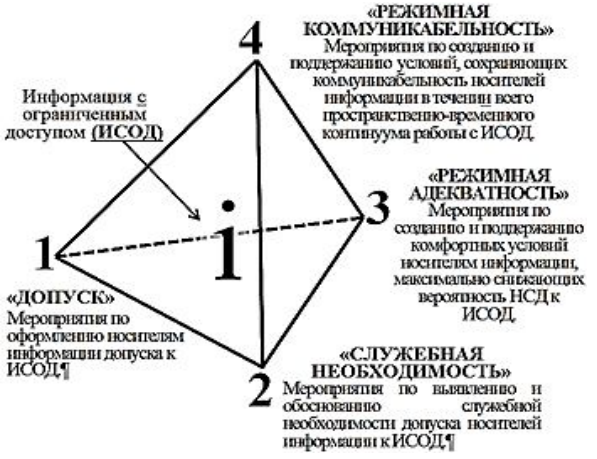

Рис. 2. Пирамида конфиденциальности.

3. При этом на выходах носителей даже, казалось бы, объективно полезные, или же просто безобидные мероприятия способны порождать трудно предсказуемые последствия.

4. Во всяком случае, нельзя искусственно добиваться полной идентичности с сигналом на входе,

поскольку, таким образом, фактически, приходится ставить граничную задачу.

5. Как следует из сказанного, очень важны сопряжения носителей, причём меры адаптационного свойства (осуществление коммуникабельности носителей информации) должны предприниматься со стороны начала каждого из последующих носителей.

Здесь напомним, что в защите информации коммуникабельность носителей вмещает элементы трёх сфер: технической, логической и социума, как это показано на рис. 3.

Рис. 3. Коммуникабельность носителей информации

Авторы [2] рассмотрели граничную задачу для системы двух дифференциальных уравнений первого порядка, отметив, что она имеет широкие приложения:

$$\begin{aligned} &d_t x(t) = a(t)x(t) + b(t)y(t); \\ &\alpha_1 x(0) + \alpha_2 y(0) = 0; \\ &d_t y(t) = c(t)x(t) + d(t)y(t) + \\ &+ f(t),\ \alpha_3 x(T) + \alpha_4 y(T) = 1, \end{aligned} \qquad (4)$$

де функции a, b, c, d, f непрерывны на $0 \le t \le T$; α_i – константы. Параметром, который используется для построения задачи Коши методом погружения, является длина интервала T.

В результате достаточно громоздких преобразований задача (4) сведена к последовательному решению четырёх задач Коши, каждая из которых представляет собой систему двух дифференциальных уравнений первого порядка [2, с. 53, 54]. На конкретном примере, продемонстрировано устранение численной неустойчивости посредством аналогичного перехода к задаче Коши [2, с. 55, 56].

В этой связи отметим также высказывание:

«С нашей точки зрения, метод инвариантного погружения позволяет заменить линейные двухточечные граничные задачи, вычислительные алгоритмы для которых часто оказываются неустойчивыми, задачами Коши, для решения которых существуют устойчивые численные методы» [5, с. 66].

Заметим, что для приведения к задаче Коши могут использоваться также методы суперпозиции, прогонки, прямого преобразования [6, пп. 2, 3, 7].

Однако в чем заключается изначальная сущность осложнений, связанных с решением задачи (4) непосредственно, как граничной?

Её объясняют тем, что в каждой из точек **t = 0** и **t = T**, по отдельности, не содержится информация, которая была бы достаточной для полного определения векторного поля **x(t), y(t).**

«С вычислительной точки зрения это соответствует ситуации, когда непосредственное применение различных схем численного интегрирования, таких как методы Рунге – Кутта, Адамса – Мултона и т. д., невозможно из-за отсутствия в начальной точке информации, необходимой для «запуска» алгоритма» [2, с. 47].

Вместе с тем, сам по себе переход к задаче Коши не решает всех проблем, поскольку может выполняться в различной интерпретации. В этой связи весьма интересны соображения А. А. Абрамова из предисловия [7]:

«Вопрос о численном решении граничных задач для систем линейных обыкновенных дифференциальных уравнений сыграл большую роль в создании современной вычислительной математики. Известны надёжные и удобные методы численного решения задачи Коши.

Естественно попытаться свести краевую задачу к нескольким вспомогательным задачам Коши. Для самых общих линейных краевых задач такое сведение кажется очевидным.

Известно, что общее решение линейной системы представляется в виде суммы какого-либо частного решения и линейной комбинации базисных решений. Все эти вспомогательные решения можно получить, решая соответствующие задачи Коши. Константы, входящие в указанное представление искомого решения, могут быть определены из системы граничных условий.

Замечательным открытием в вычислительной математике было выяснение того, что для широких классов естественных «хороших» задач упомянутый метод совершенно неприменим».

Приведём пояснение. Итак, пусть $\mathbf{u_g}$ – частное решение дифференциального уравнения второго порядка с переменными коэффициентами;

g – его свободный член; $\mathbf{u_1}$ и $\mathbf{u_2}$ – базисные решения, когда **g = 0**. Все эти функции известны.

Решение

$$u(t) = u_g(t) + c_1 u_1(t) + c_2 u_2(t); \qquad (5)$$

из граничных условий

$$\begin{aligned} &c_1 u_1(0) + c_2 u_2(0) = u(0) - u_g(0); \\ &c_1 u_1(1) + c_2 u_2(1) = u(1) - u_g(1), \end{aligned} \qquad (6)$$

где значения **u(0); u(1)** даны.

Казалось бы, можно найти $\mathbf{c_1}$ и $\mathbf{c_2}$ из системы уравнений (6). Их подстановка в (5) даст решение исходной задачи. Однако так действовать нельзя, поскольку дифференциальные уравнения в задачах Коши оказываются чувствительными к возмущениям коэффициентов, а значит, использование функций $\mathbf{u_1}$ и $\mathbf{u_2}$ не представляется возможным.

Собственно говоря, природа этой неустойчивости аналогична (3).

Приведённый материал расширяет наши представления о защите информации, особенно в ситуации, когда реализуется весьма дорогостоящий проект, к примеру, – защита государственной тайны, как информации высших ступеней секретности. Заметим, что рассмотрению упомянутой ситуации, имеющей ряд отличительных особенностей, будет посвящена другая статья авторского исследования.

Едва ли следует говорить о том, что наибольшую опасность представляет получение конкурентом информации во всем её комплексе (это является тривиальным). Не будем также затрагивать тему альтернативного проекта, являющегося «блефом» (она обсуждалась выше, п. 1.1).

Итак, «математика» показывает что, зная описание некоторого процесса и достоверные сведения о нем в некоторые моменты времени (например, данные утечки информации из компьютера в результате несанкционированного доступа (НСД) к информации - воровство протокола закрытого совещания, действия хакеров и пр.), при использовании собственником информации сугубо формализованных средств защиты (например, - дезинформации), приводит к тому, что конкурент в результате НСД получает, попросту говоря, бессмысленный результат.

Имеется в виду строгая логика умозаключений, предполагающая полную непротиворечивость накопленной информации.

С этой точки зрения, увеличение интервала времени, необходимого для получения достоверной информации ведёт к усложнению её логической обработки. Однако на некотором этапе включается совсем другой механизм, а именно – способность человека к мышлению эвристического свойства.

Здесь подразумевается иерархическая структура, отбрасывание несущественных факторов и т. п.

Вместе с тем, для того, чтобы выйти на «сценарий» работы с большим количеством «точек», очевидно, потребуются значительные средства.

Выводы

Комментарии в отношении (4) – (6) позволяют предложить стратегию:

– если конкурент несёт затраты на получение информации и потери практически неизбежны, его внимание с помощью дезинформации следует всячески привлекать на трудно стыкующиеся между собой позиции;

– подразумевается реализация эффекта парадоксальности, когда в условиях неполноты имеющейся информации, дополнительно поступающие материалы ставят под сомнение достоверность предыдущих;

– логический вывод из сказанного заключается в необходимости использования «точечной» дезинформации, которая бы препятствовала формированию у конкурента представлений целостного характера.

Список литературы

1. Громыко И.А. Будущее за упреждающими системами защиты / И.А. Громыко, С.Ю. Кильмаев, Е.Я. Оспищев // Защита информации. INSIDE. – 2007 – С. 14-18.

2. Касти Дж. Методы погружения в прикладной математике / Дж. Касти, Р. Калаба. – М.: Мир, 1976. – 225 с.

3. Ортега Дж. Введение в численные методы решения дифференциальных уравнений / Дж. Ортега, У. Пул. – М.: Наука, 1986. – 288 с.

4. Форсайт Дж. Машинные методы математических вычислений / Дж. Форсайт, М. Малькольм, К. Моулер. – М.: Мир, 1980. – 279 с.

5. Беллман Р. Динамическое программирование и уравнения в частных производных / Р. Беллман, Э. Энджел. – М.: Мир, 1974. – 208 с.

6. На Ц. Вычислительные методы решения прикладных граничных задач / Ц. На. – М.: Мир, 1982. – 204 с.

7. Тауфер И. Решение граничных задач для систем линейных дифференциальных уравнений / И. Тауфер. – М.: Наука, 1981. – 144 с.

Поступила в редколлегию 28.11.2013

Рецензент: д-р техн. наук, проф.. С.Г. Рассомахин, Харьковский национальный университет им. В.Н. Каразина, Харьков.

ЗАХИСТ ІНФОРМАЦІЇ ТА ЗАДАЧА КОШІ

І.О. Громико

У даній статті наведені рекомендації для систем захисту інформації на підставі математичної процедури приведення складної граничної задачі до задачі Коші.

Ключові слова: *захист інформації, задача Коші.*

INFORMATION PROTECTION AND SOLUTION OF THE CAUCHY

I.O. Gromyko

This article provides recommendations for information security systems based on complex mathematical procedures to bring the boundary value problem to the Cauchy problem.

Keywords: *information security, the Cauchy problem.*