УДК 004.056.5:518 Кобозева А.А., Хорошко В.А.

ИСПОЛЬЗОВАНИЕ УПРУГОЙ СИСТЕМЫ ПРИ МОДЕЛИРОВАНИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Введение

Развитие общества на современном этапе невозможно без внедрения новых информационных технологий во все сферы его жизнедеятельности.

Широкомасштабное использование вычислительной техники и телекоммуникационных систем, переход к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационных систем, к их высокой уязвимости, что необходимо влечет за собой повышение актуальности требования защищенности любой информационной системы.

Проблемы построения систем защиты информации (СЗИ) очень широко обсуждаются в современной открытой печати [1-5]. Вывод о необходимости создания системного комплексного подхода к защите информации на основе единого научного базиса [1,2] ни у кого не вызывает сомнений. Построение такого научного базиса с привлечением современных методов вычислительной математики и использованием последних достижений вычислительной техники немыслимо без наличия адекватной математической модели СЗИ, простой в вычислительном смысле, которая бы дала возможность для априорного анализа свойств системы, позволила бы оценить устойчивость СЗИ к атакам. Существующие проблемы при создании таких моделей хорошо известны [1-5] и неоднократно обсуждались авторами [6-8]. Основные из них – это сложность и разнородность информационных систем, большинство из которых плохо формализуются, требуют адаптации непосредственно в процессе функционирования и управления.

Целью настоящей работы является создание основ принципиально новой механической модели защищенной информационной системы, математическая формализация которой приводит к системе линейных алгебраических уравнений, что никогда не делалось ранее.

В качестве основных математических инструментов выступают вычислительная линейная алгебра, теория матриц, теория возмущений.

Для достижения поставленной цели необходимо решить следующие *задачи*:

- Выбрать механическую интерпретацию для СЗИ; установить соответствие между элементами информационной системы и параметрами ее механической модели;
- Провести математическую формализацию механической модели;
- Формализовать требование устойчивости СЗИ по отношению к предполагаемым атакам в рамках механической модели;
- Получить формальные условия устойчивости СЗИ к предполагаемому противнику.

2. Связь между свойствами упругой статической системы и системы защиты информации

В качестве механической модели защищенной информационной системы в силу аналогий, приведенных в табл.1, логично рассмотреть упругую статическую систему S, закрепленную на краях [9], например, стержень.

Информация, приведенная в табл.1, дает возможность для установления взаимно однозначного соответствия между элементами системы S и информационной системы.

Выберем на упругом стержне конечное множество точек, каждая из которых будет соответствовать конкретному средству защиты, имеющемуся в распоряжении информационной системы, которые для удобства занумеруем в порядке слева направо:

1,2,…,n. Будем рассматривать прогибы $b_1, b_2, ..., b_n$ точек 1,2,…,n системы S под воздействием сил $x_1, x_2, ..., x_n$, приложенных в этих точках. При этом $x_1, x_2, ..., x_n$ интерпретируются как атаки, направленные непосредственно на средства защиты 1,2,…,n, а $b_1, b_2, ..., b_n$ - результаты воздействия атак на средства защиты.

Таблица 1
Аналогии между свойствами упругой статической системы и системы защиты информации

Упругая статическая система	Система защиты информации
1. Рассчитана на определенные механические воздействия, результат которых является для системы обратимым: при снятии нагрузки (воздействия) система приходит в первоначальное положение, отвечая тем самым на воздействие.	1. Строится в соответствии с предполагаемым противником, относительно которого считается устойчивой.
2. По мере увеличения нагрузок до некоторого предела будет непрерывно увеличиваться деформация системы, не приводя к ее разрушению.	2. Предпринимаемые атаки из множества предполагаемых не наносят ущерба информации системы, хотя могут отрицательно сказаться на отдельных средствах защиты, выводя их из строя частично (или полностью). В поле таких атак СЗИ не нуждается в доработках.
3. Существуют нагрузки, превышение которых приводит к необратимой деформации системы, к ее разрушению. Система нуждается в изменении своих параметров для возможности противостоять рассмотренным нагрузкам.	3. Существуют атаки на СЗИ, не предусмотренные при ее построении, которые могут оказаться разрушительными для СЗИ: выводят из строя некоторые (все) средства защиты, результатом чего является осуществление несанкционированного доступа к информации. СЗИ нуждается в доработке.
4. Защита системы от разрушения производится за счет увеличения ее упругости при помощи изменения механических параметров, введения дополнительных опор.	4. Усовершенствование СЗИ производится при помощи активации средств защиты, введения новых средств защиты.
5. Приложение силы (нагрузки) в любой точке системы за счет ее упругости окажет воздействие на каждую точку системы.	5. Атака, предпринятая против некоторого средства защиты, так или иначе отразится на всей СЗИ, на всех ее составляющих.

3. Построение системы линейных алгебраических уравнений, отвечающей информационной системе

Предположим, что

1. Воздействующие на стержень силы и перемещения (прогибы) его составляющих перпендикулярны исходному (недиформированному) положению стержня, т.е. параллельны между собой, а значит, полностью определяются своими алгебраическими величинами (рис.1);
2. Имеет место принцип линейного наложения сил [9]:
   - при суммарном наложении двух систем сил соответствующие прогибы складываются;
   - при умножении величин всех сил на одно и то же вещественное число все прогибы умножаются на это число.

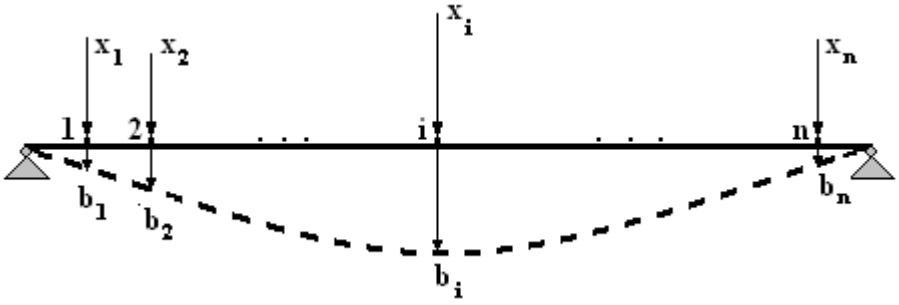

Рис.1. Деформация упругого стержня под воздействием внешних сил

Пусть a_{ik} - прогиб стержня в точке i под действием единичной силы, приложенной в точке k, или коэффициент влияния точки k на i, $i,k=\overline{1,n}$ (рис.2). При совместном действии произвольных сил $x_1, x_2, ..., x_n$ на стержень S при сделанных выше предположениях прогибы будут определяться по формуле:

$$\sum_{k=1}^{n} a_{ik} x_k = b_i, \quad i=\overline{1,n}. \tag{1}$$

Эти прогибы $b_1, b_2, ..., b_n$ являются формальной количественной интерпретацией итогового состояния каждого средства защиты после совместного проведения атак $x_1, x_2, ..., x_n$ на информационную систему.

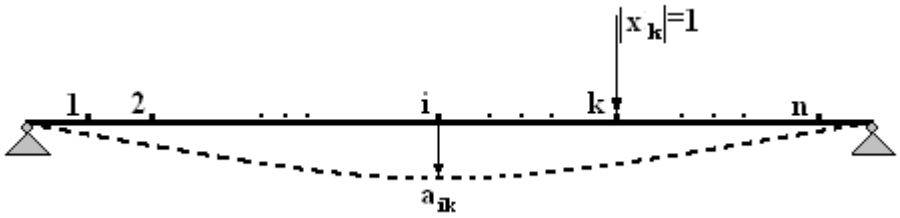

Рис.2. Определение коэффициента влияния точки k упругого стержня на точку i под воздействием единичной силы

Матричный вид соотношения (1)

$$Ax = b, \tag{2}$$

где A - $n \times n -$ матрица с элементами $a_{ik}, i,k = \overline{1,n}$, x, b - векторы длины n с элементами $x_i, b_i, i = \overline{1,n}$, соответственно.

Соотношение (2) представляет из себя в общем случае неоднородную систему линейных алгебраических уравнений (СЛАУ) относительно неизвестных воздействующих на стержень сил $x_1, x_2, ..., x_n$ при известных прогибах $b_1, b_2, ..., b_n$. Предполагая, что $\det(A) \neq 0$, имеем единственное решение (2).

Система (2) является формальным представлением СЗИ при использовании в качестве ее механической интерпретации упругого стержня. На языке теории информационной защиты задача о решении СЛАУ (2) может быть интерпретирована следующим образом: определить количественные характеристики проявления атак на защищенную информационную систему, которые приведут к определенному состоянию средств защиты. В предельном варианте: определить максимально возможные проявления атак $x_1, x_2, ..., x_n$, которые еще не приведут к разрушению СЗИ и непосредственному доступу к информации, что для задачи о деформации упругого стержня сведется к определению максимальных воздействий, которые может выдержать стержень, чтобы результат этих воздействий был обратим.

4.Условия устойчивости системы защиты информации к атакующим воздействиям

СЗИ будем называть *устойчивой* по отношению к проведенной атаке, если в результате атаки несанкционированный доступ к хранимой информации не произошел.

Назовем задачу, определяемую системой (2), *прямой.*

Механической интерпретацией устойчивости СЗИ естественно считать малые упругие изменения в деформации стержня при сравнительно большом увеличении значений воздействующих на стержень внешних сил, иначе говоря, большие возмущения $x_1, x_2, ..., x_n$ могут возникать в результате малых возмущений исходных данных $b_1, b_2, ..., b_n$. Таким образом, формально требование устойчивости СЗИ будет отражаться в требовании чувствительности [10] прямой задачи к возмущающим воздействиям.

Имеет место следующее утверждение.

Утверждение 1. Достаточным условием устойчивости СЗИ к атакам при использовании модели (2) является чувствительность задачи о решении СЛАУ (2) к возмущающим воздействиям.

Мерой чувствительности любой задачи является ее число обусловленности [11]. В случае задачи о решении СЛАУ это число обусловленности может определяться как

$$cond(A) = \|A\| \left\|A^{-1}\right\|. \tag{3}$$

Действительно [12], пусть x - точное, $\bar{x}$ - реально полученное, т.е. приближенное решение СЛАУ (2), $\delta x = \bar{x} - x$, $\delta A, \delta b$ - возмущения матрицы A и вектора b соответственно. СЛАУ (2) представляется в виде:

$$(A + \delta A)(x + \delta x) = b + \delta b \tag{4}$$

Учитывая, что $b = Ax$ и $\det(A) \neq 0$, из (4) вытекает:

$$\delta x = A^{-1}(\delta b - \delta A\bar{x}),$$

откуда получаем:

$$\|\delta x\| \le \|A^{-1}\|\left(\|\delta b\| + \|\delta A\|\|\bar{x}\|\right) = \|A^{-1}\|\|A\|\left(\frac{\|\delta b\|}{\|A\|} + \frac{\|\delta A\|\|\bar{x}\|}{\|A\|}\right).$$

Поскольку $\bar{x}$ - это решение неоднородной системы, то $\|\bar{x}\| \neq 0$. Разделив последнее неравенство на $\|\bar{x}\|$, получим:

$$\frac{\|\delta x\|}{\|\bar{x}\|} \le \|A^{-1}\|\|A\|\left(\frac{\|\delta A\|}{\|A\|} + \frac{\|\delta b\|}{\|A\|\|\bar{x}\|}\right) \qquad (5)$$

Здесь относительная погрешность результата сравнивается с относительным изменением входных данных через величину $cond(A)$, определяемую в соответствии с (3), являющуюся мерой чувствительности задачи о решении СЛАУ к возмущающим воздействиям.

В силу специфики полученной СЛАУ (2) будем считать, что $\delta A = 0$, а возмущенная система (4), для которой $\bar{x}$ является точным решением, получена лишь за счет возмущения вектора правой части. Действительно, коэффициенты матрицы A никак не зависят от изменений в x, b, они определяются лишь коэффициентом упругости стержня (мерой упругости стержня). Тогда соотношение (5) примет вид:

$$\frac{\|\delta x\|}{\|\bar{x}\|} \le cond(A)\frac{\|\delta b\|}{\|A\|\|\bar{x}\|},$$

откуда вытекает, что малые изменения в векторе прогибов b могут соответствовать большим возмущениям в векторе сил x в случае значительной величины $cond(A)$, что для моделируемой СЗИ будет отражать ее устойчивость.

Имеет место следующее утверждение.

Утверждение 2. Достаточным условием устойчивости СЗИ к атакам при использовании модели (2) является плохая обусловленность прямой задачи: $cond(A) >> 1$.

При построении механической модели защищенной информационой системы естественно считать, что СЗИ будет тем больше устойчивой к предполагаемым атакам, чем меньше будут коэффициенты влияния точек соответствующего ей упругого стержня друг на друга, т.е. чем меньше будут коэффициенты матрицы A, чем больше будет коэффициент упругости стержня. Очевидно, при построении механической модели гипотетически идеальным с точки зрения устойчивости СЗИ будет вариант, когда $a_{ik} = 0,\ i,k = \overline{1,n}$, тогда все прогибы $b_1, b_2, ..., b_n$ будут нулевыми независимо от конкретного проявления сил. В этом случае $cond(A) = \infty$. Однако на практике это очевидно является нереальным.

Заметим, что даже, если $A \neq 0$, но $\det(A) = 0$ ($cond(A) = \infty$), то нулевой вектор b в прямой задаче (2) может отвечать ненулевому вектору воздействующих на стержень сил x, что говорит в пользу адекватности предлагаемой модели СЗИ. Действительно, упомянутый случай является интерпретацией существования для СЗИ таких атак, воздействие которых никак не скажется на средствах защиты и, как следствие, на самой информации.

Однако в реальных условиях для устойчивой СЗИ логично предположить, что

$$a_{ik} \approx 0,\ i,k = \overline{1,n}. \qquad (6)$$

С большой вероятностью при выполнении условий (6) элементы A будут мало отличаться по значениям друг от друга. Тогда даже если $\det(A) \neq 0$, значение определителя может оказаться близким к нулю. Действительно, малые отличия a_{ik} между собой приведут к малой мере линейной независимости между векторами-столбцами (векторами-строками) матрицы A - малым углам между ними (рис.3). Близость определителя матрицы к нулю приведет к большому значению числа обусловленности $cond(A)$, а значит к чувствительности прямой задачи к возмущающим воздействиям. Это позволяет говорить об истинности следующего утверждения.

Утверждение 3. Пусть СЗИ является устойчивой к предполагаемым атакам, тогда с большой вероятностью соответствующая ей СЛАУ (2) будет чувствительной к возмущающим воздействиям.

Утверждение 3 дает формальное необходимое условие устойчивости СЗИ к предполагаемым атакам и в сочетании с утверждением 2 позволяет сформулировать следующий критерий.

Теорема. Для того, чтобы СЗИ при ее формальном представлении в виде СЛАУ (2) была устойчивой к предполагаемым атакам необходимо и достаточно, чтобы прямая задача была чувствительной к возмущающим воздействиям, т.е. чтобы матрица СЛАУ (2) была плохо обусловлена: $cond(A) >> 1$.

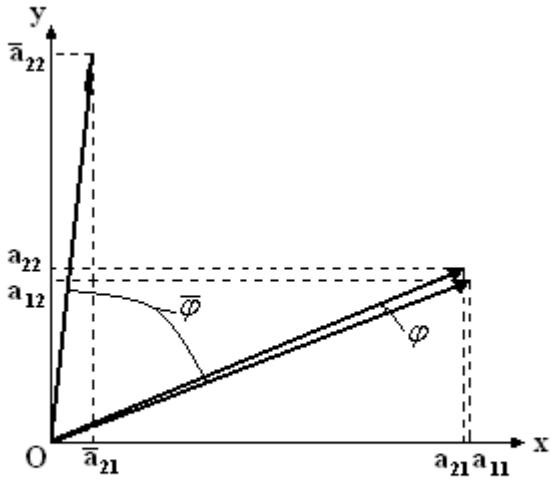

Рис.3. Различные меры линейной независимости между векторами-столбцами A при $n = 2$

Заметим, что прямая задача рассматривалась нами только с точки зрения решения вопроса об устойчивости СЗИ: фигурирующие возмущения вектора правой части b предполагались малыми.

Предположим, что в результате атак несанкционированный доступ к информации произошел. Это означает, что СЗИ не являлась устойчивой к предпринятым противником атакам, она нуждается в дополнительной доработке, «укреплении», которое формально может выглядеть следующим образом.

Система S заменяется статической упругой системой S_p, полученой из S введением p неподвижных шарнирных опор в p точках ($p \leq n$) [9]. Не ограничивая общности, для простоты изложения будем считать, что опоры введены в точках $1,\ldots,p$. Коэффициенты влияния для оставшихся подвижных $n-p$ точек $p+1,\ldots,n$ системы S_p будем обозначать через $a_{ik}^{(p)},\ i,k = \overline{p+1,n}$, (рис.4 для $p = 1$).

Коэффициент $a_{ik}^{(p)}$ можно рассматривать как прогиб в точке i системы S при действии единичной силы в точке k и сил реакций $r_1, r_2, \ldots, r_p$ в точках $1,\ldots,p$. Поэтому

$$a_{ik}^{(p)} = a_{ik} + r_1 a_{i1} + \ldots + r_p a_{ip}. \qquad (7)$$

Прогибы системы S при этих же силах в точках $1,\ldots,p$ равны нулю, что эквивалентно

$$\begin{cases} r_1 a_{11} + \ldots + r_p a_{1p} + a_{1k} = 0, \\ r_1 a_{21} + \ldots + r_p a_{2p} + a_{2k} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_1 a_{p1} + \ldots + r_p a_{pp} + a_{pk} = 0. \end{cases} \qquad (8)$$

Матрица системы (8), которую обозначим $A^{(p)}$, является главной подматрицей порядка p матрицы A исходной СЛАУ (2). Если

$$\det\left(A^{(p)}\right) \neq 0, \qquad (9)$$

то из (8) однозначно определяются значения $r_1, r_2, \ldots, r_p$. При подстановке полученных $r_1, r_2, \ldots, r_p$ в (7), получаем значения $a_{ik}^{(p)}$- новые прогибы «усовершенствованной» упругой системы, определяющие новые результаты воздействий атак на средства защиты «усовершенствованной» СЗИ.

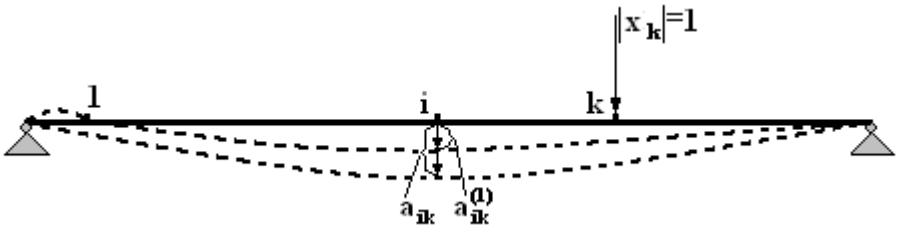

Рис.4. Деформация упругого стержня под воздействием единичной силы при наличии дополнительной опоры

Замечание 1. При адекватном моделировании СЗИ необходимо учитывать возможность возникновения атак, не предусмотренных при первоначальном конструировании СЗИ. При рассмотренном в работе способе построения модели это возможно проделать следующим образом: при механической интерпретации СЗИ не обязательно предполагать, что точки, в которых рассматриваются прогибы (отвечающие конкретным средствам защиты), совпадают с точками приложения сил $x_1, x_2, \ldots, x_n$. Можно рассмотреть вариант, когда $b_1, b_2, \ldots, b_n$ - прогибы точек $1,2,\ldots,n$, а силы приложены в точках $1',2',\ldots,n'$, причем i и i' могут как совпадать, так и не совпадать ($i = \overline{1,n}$). Несовпадение точки приложения i' силы x_i с точкой i и будет моделировать непредусмотренную атаку. В этом случае a_{ik} - коэффициент влияния точки k' на точку i, а вместо опоры в точке j можно рассматривать «обобщенную опору» [9] в точках j, j', при которой прогиб в точке j поддерживается все время равным нулю, если надлежащим образом выбрать силу r_j в точке j'. Условие возможности введения p обобщенных опор в точках $1,1';\ 2,2';\ \ldots;\ p, p'$, т.е. возможность удовлетворить условиям $b_1 = 0, b_2 = 0, \ldots, b_p = 0$ при любых $x_{p+1}, \ldots, x_n$ путем выбора надлежащих $r_1 = x_1, \ldots, r_p = x_p$, выражается неравенством (9).

Замечание 2. «Укрепление» СЗИ формально может быть проведено за счет увеличения коэффициента упругости системы S, что будет отвечать росту чувствительности прямой задачи, увеличению $cond(A)$.

Замечание 3. Рассмотрение в качестве механической модели защищенной информационной системы упругого стержня является первым шагом на пути построения механической модели. Более привлекательной в этом отношении является рассмотрение упругой пластины, для которой соответствующая система уравнений может быть получена, например, с привлечением метода конечных элементов, различных схем смешанного метода конечных элементов.

Замечание 4. Рассматривая в качестве модели СЗИ краевую задачу об изгибе пластины, защищенность информационной системы, а также ее адекватность, определяемая как обеспечение требуемого уровня защиты при минимальных издержках на создание механизма защиты и обеспечение его функционирования, может интерпретироваться за счет выбора конкретного вида краевых условий.

5.Заключение

На основании проделанной работы можно утверждать, что предлагаемый новый подход к вопросу моделирования СЗИ, основанный на аналогиях между упругой статической системой и системой информационной безопасности, использующий в качестве математических инструментов матричный анализ, вычислительную линейную алгебру, теорию возмущений, является чрезвычайно перспективным.

Задачи, поставленные в работе, решены полностью, цель достигнута.

Литература:

1. Хорошко В.А. Методы и средства защиты информации / В.А.Хорошко, А.А.Чекатков. — К.: Юниор, 2003. — 501 с.
2. Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. — К.: Арий, 2008.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / Домарев В.В. — Изд-во: ТИД «ДС», 2001. — 688с.
4. Домарев В.В. Безопасность информационных технологий. Системный подход / Домарев В.В. — Изд-во: ТИД «ДС», 2004. — 992с.
5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / Малюк А.А. — М.: Горячая линия — Телеком, 2004. — 280с.
6. Кобозева А.А. Модель системы защиты информации, основанная на принципах естественной системы управления / А.А.Кобозева, В.А.Хорошко // Захист інформації. - 2007. – Спецвипуск. - С.56-62.
7. Кобозева А.А. Методика оценки адекватности системы защиты информации / А.А.Кобозева, В.А.Хорошко // Вісник ДУІКТ. - 2007. - №5(3). - С.328-334.
8. Кобозева А.А. Векторная sign-чувствительность как основа геометрической модели системы защиты информации / А.А.Кобозева, В.А.Хорошко // Захист інформації. – 2008. - №3 - С. 49-57.
9. Гантмахер Ф.Р. Теория матриц / Ф.Р.Гантмахер. — М.: Наука, 1988. — 552 с.
10. Деммель Дж. Вычислительная линейная алгебра / Дж.Деммель; пер. с англ. Х.Д.Икрамова. — М.: Мир, 2001. — 430 с.
11. Кобозева А.А. Общий подход к анализу состояния информационных объектов, основанный на теории возмущений / А.А.Кобозева // Вісник Східноукраїнського національного університету ім. В.Даля. – 2008. - №8(126),ч.1. - С.72-81.
12. Кобозева А.А. Стеганографический метод, основанный на решении системы линейных алгебраических уравнений / А.А.Кобозева, А.В.Коломийчук // Праці УНДІРТ. – 2006. - №1(45)-2(46). - С.104-109.

АНОТАЦІЯ

УДК 004.056.5: 518

Кобозєва А.А., Хорошко В.О. Використання пружної статичної системи при моделюванні системи захисту інформації.

В роботі запропоновано основи принципово нової моделі захищеної інформаційної системи, заснованої на механічній інтерпретації системи лінійних алгебраїчних рівнянь із залученням теорії збурень, що ніколи не робилося раніше.

Літ. 12 назв., іл. 4.

«Захист інформації»,2009, №2, с.11-18.