Список літератури

1. *Сбитнев А.И.* Структурные методы проектирования математического обеспечения АСУ ТП// Модели и алгоритмы автоматизированных систем в промышленности. – К.: ИК АН УССР, 1982. – С. 3-9.
2. *Лєнков С.В., Вишнівський В.В., Перегудов Д.О., Толюпа С.В.* Методика розрахунку часу затримки інформації управління в мережах при випадковому потоці повідомлень // Вісник державного університету інформаційно-комунікаційних технологій. – К., 2007.- №5(4). – С. 10 – 18.
3. *Грищак О.М.* Пропозиції до перспективної структури підрозділу, що розробляє спеціальне програмне забезпечення военного призначення // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2007. – № 8. – С.61 -66.

Надійшла 26.03.2008р.

УДК 004.056.5: 518

А.А.Кобозева, В.А Хорошко

ВЕКТОРНАЯ SIGN-ЧУВСТВИТЕЛЬНОСТЬ КАК ОСНОВА ГЕОМЕТРИЧЕСКОЙ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Введение

Процесс внедрения новых информационных технологий во все сферы жизни общества немыслим без решения вопросов информационной безопасности. Современное общество вступает в постиндустриальный период своего развития, который по всеобщему мнению можно назвать информационным [1].

Создание интенсивной системы комплексного обеспечения безопасности информационных технологий невозможно без обобщения накопленного опыта теоретических исследований и практического решения задач защиты информации, т.е. без развитого научного базиса [2,3], создание которого немыслимо без разработки адекватной математической модели системы защиты информации (СЗИ). В современных публикациях данному вопросу уделено много внимания [2,4-6], однако предложенные формализации не удовлетворяют всем выдвигаемым к математической модели СЗИ требованиям, являются, как правило, достаточно сложными в вычислительном смысле [5,6], что безусловно связано с тем, что теоретические основы построения СЗИ исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства [2].

В [7] предложена модель СЗИ, основывающаяся на принципах функционирования нервной системы человека. Математическими инструментами для ее создания явились теория графов, матричный анализ и теория возмущений. Применение теории возмущений позволило производить априорную оценку адекватности моделируемой СЗИ предполагаемому противнику [8], дало возможность для определения чувствительности совокупной системы к возмущающим воздействиям (атакам). Настоящая работа является дальнейшим развитием предложенного в [7] подхода, использующего чувствительность информационного объекта для определения его свойств.

Любая атака, действующая на информационно-технологическую систему (ИТС), на каждом из имеющихся в распоряжении СЗИ средств защиты отразится по-разному: некоторые из средств могут быть разрушены полностью, некоторые выведены из строя частично, а для каких-то средств атака окажется безопасной.

Целью настоящей работы является создание основ модели СЗИ, дающей возможность простого в вычислительном смысле учета различий в результатах воздействия атаки для разных средств защиты, следствием чего в перспективе должно стать значительное упрощение решения задачи по установлению адекватности СЗИ предполагаемому противнику по

обміну інформацією. Ще чотири провідника залишаються вільними і можуть бути використані для побудови системи контролю розкриття апаратури. Використання незадіяних в передачі даних провідників також не створює завади передачі даних, що не зменшує продуктивність мережі в цілому.

Другий напрямок використання цієї концепції полягає в наступному. Фізична безпека взагалі будь-яких матеріальних носіїв інформації комп'ютерної системи, а не тільки її ядра безпеки у вигляді комплексу засобів захисту, може забезпечуватись шляхом їх радіоізотопного маркування.

У світовій практиці за останні роки для маркування носіїв інформації, цінних предметів, паперів, пластикових кредитних карток все частіше використовують радіоактивні речовини [4-7]. Сутність методу, запатентованого в США, полягає у введенні радіоактивного ізотопу відповідної активності в структуру предмету, що маркується [6].

Активність мітки, тип ізотопу, її координати є ідентифікаційними параметрами і заносяться до спеціального каталогу. До недоліків даного методу можна віднести: необхідність звернення до каталогу, корекцію на розпад ізотопу, невисоку точність вимірювання остаточної активності і, як наслідок, збільшення часу ідентифікації та можливість втрати мітки.

Сутність методу, запатентованого у Франції [7], полягає у введенні радіоактивного ізотопу в спеціально просвердлений канал предмету, що маркується, з наступним його маскуванням. Недоліком даного методу є [4]:

досить висока активність і вид випромінювання (рентгенівське або гама-випромінювання) в залежності від матеріалу предмету;

можливість знайдення мітки;

руйнація структури об'єкту, що маркується, та недостатність ідентифікаційних ознак;

можливість підробки.

У концепції запропоновано використання β-випромінювань, які знайшли поширене використання в техніці та промисловості завдяки:

простим детекторам зчитування випромінювання майже із 100% ефективністю;

досить великій кількості поєднань виробів з радіонуклідами;

наявності "чистих" колімованих бета-мікровипромінювачів з довжиною контейнера 2.8 мм, діаметром 0.8 мм, діаметром колімаційного отвору 0.4 мм;

більш безпечному для здоров'я людини, аніж гама або нейтронне;

відсутності складних пристосувань для захисту від випромінювання.

Використання радіоізотопного маркування забезпечує контроль і захист визначених матеріальних носіїв інформації комп'ютерної системи від підмін, викрадень тощо [4-5]. Для цього концепцією регламентуються спеціальні методи, способи та засоби (технології) радіоізотопного маркування визначених політикою фізичної безпеки апаратних засобів комп'ютерної системи. Радіоізотопні коди-мітки за вимогами цієї концепції повинні бути латентним (прихованими), кодованими в декілька рівнів їх захищеності (геометрична форма мітки, місце розташування, виявлення на певній відстані, тип радіоізотопу тощо), а також бути екологічно безпечними. Коди-мітки - це розроблена у Державному науково-дослідному інституті внутрішніх справ України радіоізотопна технологія захисту носіїв інформації та предметів. Це абсолютно нові (отримано патенти на винаходи) методи, способи та засоби захисного маркування з використанням безпечних для здоров'я людини слаборадіоактивних ізотопів. Захисне маркування базується на введенні у звичайну типографську фарбу препаратів-носіїв спеціально підібраних слаборадіоактивних ізотопів та зчитуванні цих маркувань (спеціальними приладами індикаторного портативного типу двох рівнів: за принципом „свій-чужий" та спеціального ідентифікаційного коду з розшифровкою та винесенням на монітор усієї необхідної інформації.

Третій напрямок практичного використання цієї концепції полягає в тому, що забезпечення безпеки фізичного стану здоров'я користувачів при роботі за комп'ютером

сравнению с [7]. Для максимального упрощения модели, увеличения ее наглядности, иллюстративности выбран геометрический способ представления.

Для достижения поставленной цели необходимо решить следующие *задачи*:

- определить такой математический параметр, характеризующий информационный объект при его используемом математическом представлении, качественное изменение которого различно в зависимости от характера (геометрически – от направления) возмущающего воздействия;
- выбрать способ для определения координат геометрических составных частей совокупной модели СЗИ таким образом, чтобы, во-первых, эти координаты несли смысловую нагрузку, определяя свойства тех информационных объектов, математическими моделями которых являются соответствующие геометрические объекты, во-вторых, способ определения координат должен обеспечить разную качественную картину их возмущений для различных геометрических объектов, а значит, для соответствующих информационных объектов, при одном возмущающем воздействии;
- выбрать способ моделирования атак на ИТС таким образом, чтобы он позволял отразить не только непосредственную направленность атаки, но чтобы и способ представления результата атаки в вычислительном смысле был как можно более простым.

2. Понятие sign-, nsign-чувствительности математического объекта

Вопросы чувствительности задачи в любой области знаний, в том числе и в области информационной безопасности, играют важную роль при оценке погрешности ее решения. В общем случае задача называется *чувствительной* к возмущениям (погрешностям исходных данных), если даже малые возмущающие воздействия (малые погрешности исходных данных) могут привести к значительной погрешности результата, и *нечувствительной* в противном случае [9]. Большая чувствительность задачи лишает даже потенциальной возможности получения ее результата с допустимой погрешностью [10].

Определение 1. Чувствительностью информационного объекта в общем случае назовем чувствительность задачи его формирования.

Наряду с оценкой классической чувствительности для всестороннего анализа результата некоторых задач из области информационной безопасности значимой также будет оценка знаковой, или sign-чувствительности, которая уже затрагивалась в [11,12].

Определение 2. Математический объект, элементами которого являются действительные числа, будем называть *sign-чувствительным*, если даже малые возмущающие воздействия могут привести к изменению знаков элементов объекта, и *sign-нечувствительным* в противном случае.

Очевидно, что sign-чувствительность (ЗЧ) (sign-нечувствительность (ЗНЧ)) любого объекта сведется к ЗЧ (ЗНЧ), соответствующей определению 2, его скалярных составляющих элементов. Естественно полагать, что чем больше sign-чувствительных скалярных элементов в составе объекта, тем более этот объект sign-чувствительный в целом.

Рассмотрим пространство произвольной размерности R^n, где R - множество действительных чисел, и определим достаточные условия ЗЧ его элементов – точек (векторов) вида $x = (x^1, x^2, ..., x^n)^T$.

Пусть $x \in R^n$. Любое возмущение для точки x можно представить как ее параллельный перенос, изменяющий в общем случае все ее координаты, что приведет к изменению длины и повороту вектора $x = (x^1, x^2, ..., x^n)^T$ на некоторый угол. В соответствии с определением 2 о sign-чувствительности x будет говорить наличие малых по абсолютной величине значений ее координат. Если у $x = (x^1, x^2, ..., x^n)^T$ имеется только одна компонента x^j, для которой $|x^j| << 1$, то перевести x в другой координатный ортант, изменив знак x^j, в состоянии малые

возмущающие воздействия, выражением которых являются параллельные переносы на малые расстояния, вектора которых параллельны координатной оси, соответствующей x^j, либо составляют с этой осью малый угол или угол, близкий к развернутому. Если же малых по абсолютной величине компонент у точки x больше одной, то больше будет и возможностей для различных проявлений возмущающих воздействий (геометрически – различных направлений параллельных переносов), результатом чего явится переход x в отличный от первоначального координатный ортант. Вследствие этого естественно считать, что чем больше малых по модулю координат в составе $x = (x^1, x^2, ..., x^n)^T$, тем более sign-чувствительной будет точка (вектор) x. Таким образом имеет место следующее утверждение.

Утверждение 1. Достаточным условием sign-чувствительности произвольного вектора $x \in R^n$ является малость $\|x\|_1$, где $\|\bullet\|_1$ - векторная 1-норма [13]. Мерой sign-чувствительности $x \in R^n$ к возмущающим воздействиям может выступать величина $\|x\|_1$: чем меньше $\|x\|_1$, тем более sign-чувствительным будет x.

Очень часто при работе с векторами, когда они используются в качестве математического инструмента для анализа свойств реальных объектов, прибегают к их нормированию, что позволяет достичь бóльшей определенности в описании вектора, его геометрическом расположении, уменьшить объем исследуемой информации, удаляя из рассмотрения одну из векторных характеристик – длину, а также дает возможность в некоторых случаях уйти от неоднозначности объектов, определяемых векторами (так поступают, например, при определении сингулярных, сообственных векторов матриц, получаемые при соответствующих разложениях). В силу этого конкретизируем понятие ЗЧ для нормированных векторов.

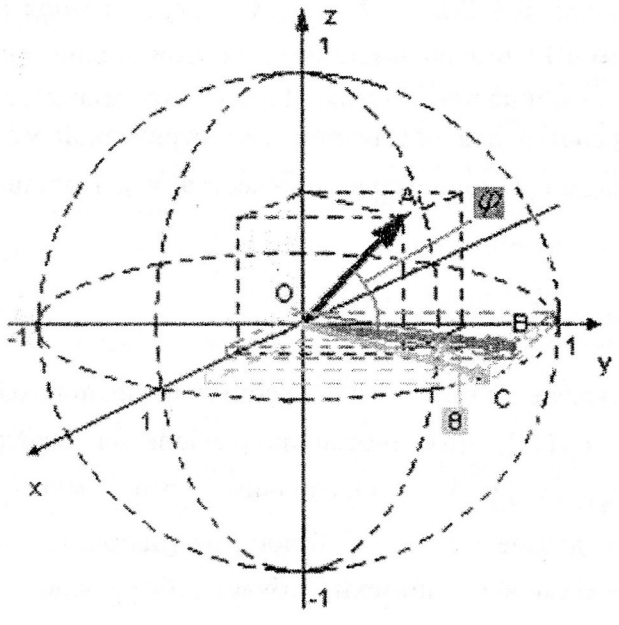

Рисунок 1. Геометрическая интерпретация nsign-чувствительности

Пусть вектор $x \in R^n$, $\|x\| = 1$ (если это не так, то предварительно нормируем его). Для наглядности изложения в качестве векторной нормы здесь рассматривается норма Фробениуса [13], хотя может использоваться и любая другая. Результатом произвольного возмущающего воздействия для нормированного вектора является его поворот на некоторый угол, а ЗЧ геометрически означает, что он составляет малый угол (углы) с координатной плоскостью (плоскостями) (вектор $\overrightarrow{OB}$ на рис.1 ($n = 3$)), о чем свидетельствует малость модулей его некоторых координат *по сравнению* с другими координатами. Назовем ЗЧ, характеризующую нормированные вектора, nsign-чувствительностью (НЗЧ).

Утверждение 2. Достаточным условием nsign-нечувствительности (НЗНЧ) вектора $x \in R^n$ является сравнимость между собой значений модулей всех его координат (малый разброс этих значений в сегменте [0,1]), что геометрически соответствует сравнимости всех углов между вектором и координатными плоскостями. Чем меньше разброс значений модулей координат вектора в сегменте [0,1], тем он менее nsign-чувствительный. Наименьшей nsign-чувствительности отвечает равенство всех координат вектора (равенство всех углов между вектором и его проекциями на координатные плоскости).

Определение 3. Нормированный вектор $\bar{x} = \left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, ..., \frac{1}{\sqrt{n}}\right)^T$, обладающий наименьшей НЗЧ, назовем *n-оптимальным.*

Заметим, что указать вектор, который бы обладал наименьшей ЗЧ, очевидно невозможно.

Замечание 1. ЗЧ и НЗЧ могут не соответствовать одна другой для одного и того же вектора $x \in R^n$. Например, если $x = (\varepsilon, \varepsilon, ..., \varepsilon)^T \in R^n$, где $|\varepsilon| << 1$, то $\|x\|_1 = n|\varepsilon|$ может быть сколь угодно малой, т.е. такой вектор x будет sign-чувствительным к возмущающим воздействиям, однако при его нормировании получим n-оптимальный вектор $\bar{x}$. Очевидно, что если координаты вектора $x \in R^n$ малые, но сравнимые между собой, то такой вектор всегда будет sign-чувствительным и nsign-нечувствительным одновременно.

В отличие от классической чувствительности, sign-чувствительный (nsign-чувствительный) вектор может не проявить свою знаковую чувствительность, даже претерпев большое возмущение ($\overrightarrow{OA}$ - результат возмущения nsign-чувствительного вектора $\overrightarrow{OB}$ (рис.1)). Для реакции sign-чувствительного вектора на возмущение важно геометрическое направление этого возмущения при его математическом представлении, т.е. проявление или непроявление последствий ЗЧ, НЗЧ в виде изменения знака координат будет зависеть от конкретики возмущающего воздействия.

Таким образом, математический параметр, качественное изменение которого различно в зависимости от характера возмущающего воздействия, найден.

3. Построение геометрической модели СЗИ

Пусть множество средств защиты, входящих в ИТС, - $X = \{x_1, x_2, ..., x_m\}$, а множество возможных атак – $V' = \{V_1', V_2', ..., V_l'\}$. Выделим в V' независимые между собой атаки: никакая из них не может быть представлена как комбинация других. Пусть это множество - $V = \{V_1, V_2, ..., V_n\}$. Выберем в качестве пространства для построения геометрической модели СЗИ пространство R^n (его размерность совпадает с мощностью множества V). Поставим в соответствие $V_i \in V$ одноименный вектор

$$V_i = ae_i, i = \overline{1,n}, \qquad (1)$$

где $-1 \le a < 0$ - параметр, выбор которого обсуждается ниже, а e_i - вектор стандартного базиса R^n. Любая атака $V_i \in V$, предпринимаемая на ИТС, практически направлена на некоторые определенные средства защиты $\{x_{i_1}, x_{i_2}, ..., x_{i_k}\} \subseteq X$. Обозначим это множество $\{x_{i_1}, x_{i_2}, ..., x_{i_k}\} = \overline{X}_i$. Если средство $x_j \notin \overline{X}_i$, то для него атака V_i безопасна (например, атака, направленная на выведение из строя шумовой помехи, будет безопасной для криптографических средств защиты).

Первоначально в качестве модели СЗИ рассмотрим совокупность m векторов пространства R^n, каждый из которых отвечает конкретному средству защиты, входящему в состав рассматриваемой ИТС. Для непосредственного определения координат вектора используем подход, основанный на учете его sign-чувствительности.

Для каждого средства защиты x_i определим множество «опасных» для него атак, т.е. всех таких атак $V_j \in V$, что $x_i \in \overline{X}_j$. Обозначим это множество $\overline{V}_i = \{V_{i_1}, V_{i_2}, ..., V_{i_t}\}$, а $\overline{\overline{V}}_i = V / \overline{V}_i$. Тогда координаты одноименного вектора $x_i = \left(x_i^1, x_i^2, ..., x_i^n\right)$, отвечающего средству $x_i \in X$, определяться следующим образом:

$$x_i^j = \begin{cases} \varepsilon, \text{ если } V_j \in \overline{V}_i, \\ 1, \text{ если } V_j \in \overline{\overline{V}}_i \end{cases}, \quad j = \overline{1,n},$$

где $0 < \varepsilon << 1$. Для каждого средства защиты x_i значения координат соответствующего вектора явно указывают на атаки, направленные против x_i.

Первоначально каждый вектор x_i находится в первом координатном ортанте, однако в соответствии с определением 1, применяемым к скалярному объекту, различные координаты вектора имеют разную ЗЧ. Для большей наглядности и удобства дальнейшего изложения построим в R^n выпуклый многогранник (в вырожденном случае – выпуклый многоугольник) S так, чтобы каждая из его вершин совпадала с концом одного из векторов $x_1, x_2, ..., x_m$, а концы векторов, не являющихся вершинами, принадлежали внутренности [14] S. Многогранник S вместе с построенными первоначально векторами $x_1, x_2, ..., x_m$ будем рассматривать в качестве геометрической модели СЗИ и обозначать $GM1$. Результат любой атаки V_i естественно формализовать при помощи параллельного переноса S вместе с концами векторов $x_1, x_2, ..., x_m$ вдоль вектора $V_i = ae_i$. Такой способ моделирования не только чрезвычайно прост, он по смыслу соответствует тому, что на самом деле атака всегда направлена против ИТС в целом, а ее непосредственное воздействие на конкретные средства защиты – это лишь способ проявления. Кроме того, при учете ЗЧ координат векторов $x_1, x_2, ..., x_m$ результат действия определенной атаки будет принципиально отличаться для разных средств защиты: могут «пострадать», изменив знак своих координат и содержащий их координатный ортант, вектора, отвечающие тем средствам, для которых соответствующая атака была «опасной». В то же время, вектора, отвечающие средствам, для которых данная атака была безопасной, хоть и возмутятся, но останутся в пределах первоначального ортанта. Заметим, что в общем случае, углы отклонения различных векторов $x_1, x_2, ..., x_m$, входящих в состав модели $GM1$, от своего первоначального положения вследствии атаки будут различны.

Как уже было отмечено выше, в общем случае предпринятая против конкретного средства защиты x_i атака V_j, $V_j \in \overline{V}_i$, может либо полностью уничтожить его, либо вывести из строя частично, лишь ослабив его защитные свойства. Моделирование уничтожения x_i, происходящее за счет перехода вектора, отвечающую атакованному средству, в отличный от первоначального координатный ортант, достигается путем параллельного переноса S на вектор $V_j = ae_j$, длина которого $|a|$ больше ε. При частичном выведении из строя x_i длина вектора параллельного переноса, соответствующего этой атаке, должна быть меньше ε, что в итоге увеличит меру sign-чувствительности вектора x_i, оставляя его в пределах исходного ортанта. Возможно степень частичного разрушения имеет несколько градаций, что повлечет за собой различие в длине вектора $V_j = ae_j$ параллельного переноса для S при моделировании различных проявлений этой атаки. Заметим, что в результате предпринятой атаки V_j изменится лишь одна j-ая координата векторов $x_1, x_2, ..., x_m$, входящих в $GM1$, став равной $\overline{\overline{x}}_i^{(j)} = x_i^{(j)} + a$, все остальные координаты останутся без изменения. Таким образом, имеет место следующее утверждение.

Утверждение 3. Вычислительные затраты для моделирования результата предпринятой на ИТС атаки при использовании $GM1$ составляют m арифметических операций, т.е. определяются лишь количеством имеющихся средств защиты, не зависят от вида атаки.

Предложенный способ построения $GM1$ чрезвычайно удобен для отражений в уже существующей модели изменений в СЗИ, а также во множестве V. Рассмотрим подробно такие модификации.

1. Добавление в ИТС новых средств защиты приведет лишь к механическому добавлению новых векторов в уже существующую геометрическую модель, которое никак не затронет построенные ранее $x_1, x_2, ..., x_m$.

2. Пусть на ИТС предпринимается атака, отсутствующая во множестве $V = \{V_1, V_2, ..., V_n\}$, но являющаяся комбинацией некоторых элементов V. Моделирование такой атаки осуществляется на основе элементарных векторных операций. Пусть, например, на СЗИ предпринимается атака, являющаяся некоторой комбинацией V_1, V_3. Тогда эта атака может быть геометрически смоделирована в виде линейной комбинации соответствующих векторов V_1, V_3: $W = \alpha e_1 + \beta e_3$, где α, β несут информацию о конкретном проявлении каждой из атак V_1, V_3 (играют роль параметра a в (1)). Вектор W определит параллельный перенос для S. По сути атака W в данном случае может рассматриваться как последовательное применение атак V_1, V_3, и хотя в реальности разделение по времени между V_1, V_3 может отсутствовать, геометрически результат будет абсолютно аналогичен в силу выбранного способа моделирования атаки.

3. Пусть на СЗИ направлена атака U, которая не принадлежит множеству V и не может быть представлена как комбинация элементов этого множества. «Пополнение» множества V атакой U отразиться на модели СЗИ. Во-первых, такое пополнение должно перевести модель из пространства R^n в пространство R^{n+1}, во-вторых, изменить непосредственные координаты векторов $x_1, x_2, ..., x_m$ геометрической модели $GM1$. Рассмотрим подробно процесс модификации модели СЗИ в этом случае.

Обозначим $U = V_{n+1}$. Пусть атака U направлена на средства защиты $x_{u_1}, x_{u_2}, ..., x_{u_k}$, составляющие множество $\overline{X}_{n+1}$, а для других средств она безопасна. Для отражения возможности возникновения такой атаки первоначально модель $GM1$ строится не в пространстве R^n, а сразу в пространстве R^{n+1}, в плоскости $x^{n+1}=1$. Это обеспечит равенство 1 последней координаты всех векторов $x_1, x_2, ..., x_m$: первоначально, пока атака U не принадлежит множеству V' как потенциально возможная для рассматриваемой ИТС, она безопасна для всех средств защиты. Введение атаки U во множество V вызовет изменение последней координаты только для точек, отвечающих средствам защиты из множества $\overline{X}_{n+1}$, что потребует точно $k \le m$ арифметических операций. Эта координата станет равной ε, что завершит процесс модификации первоначальной геометрической модели.

Учет возможности появления нескольких новых атак $U_1, U_2, ..., U_t$ проводится совершенно аналогично вышесказанному, только исходная модель СЗИ первоначально строится не в пространстве R^n, а сразу в пространстве R^{n+t}, при этом t последних координат всех векторов $x_1, x_2, ..., x_m \in R^{n+t}$ первоначально полагаются равными 1.

Для случая $n = 3$, $m = 3$ наглядная иллюстрация геометрической модели СЗИ без учета возможности возникновения новых атак приведена на рис.2. Вследствие предпринятой атаки V_2 вышло из строя средство x_2, о чем сигнализирует вектор, отвечающий этому средству, оказавшийся в другом координатном ортанте (на рис.2 он выделен красным цветом). Эта же атака не сказалась разрушительно на оставшихся средствах защиты x_1, x_3.

Если в основу построения геометрической модели СЗИ положить НЗЧ, т.е. предварительно нормировать вектора $x_1, x_2, ..., x_m$, соответствующие средствам защиты, результатом чего будут вектора $x_1', x_2', ..., x_m'$, то модель, отвечающая представленной на рис.2, будет иметь вид, изображенный на рис.3. Далее геометрическую модель, основанную на НЗЧ векторов, будем обозначать $GM2$. Заметим, что многогранник (многоугольник) S перейдет в некоторую связную n-мерную поверхность, являющуюся частью n-мерной сферы, что геометрически является более предпочтительным с точки зрения удобства обработки и анализа

геометрического объекта. Моделирование атаки V_i в силу нормированности $x_1', x_2', ..., x_m'$ удобнее проводить при помощи поворота совокупной модели $GM2$ на угол, плоскость которого параллельна координатной оси, соответствующей i-ой координате вектора. Таким образом, результатом атаки является поворот всех векторов $x_1', x_2', ..., x_m'$, входящих в модель $GM2$, на один и тот же угол. Переход вектора в другой координатный ортант в силу его НЗЧ будет сигнализировать о разрушении соответствующего средства защиты.

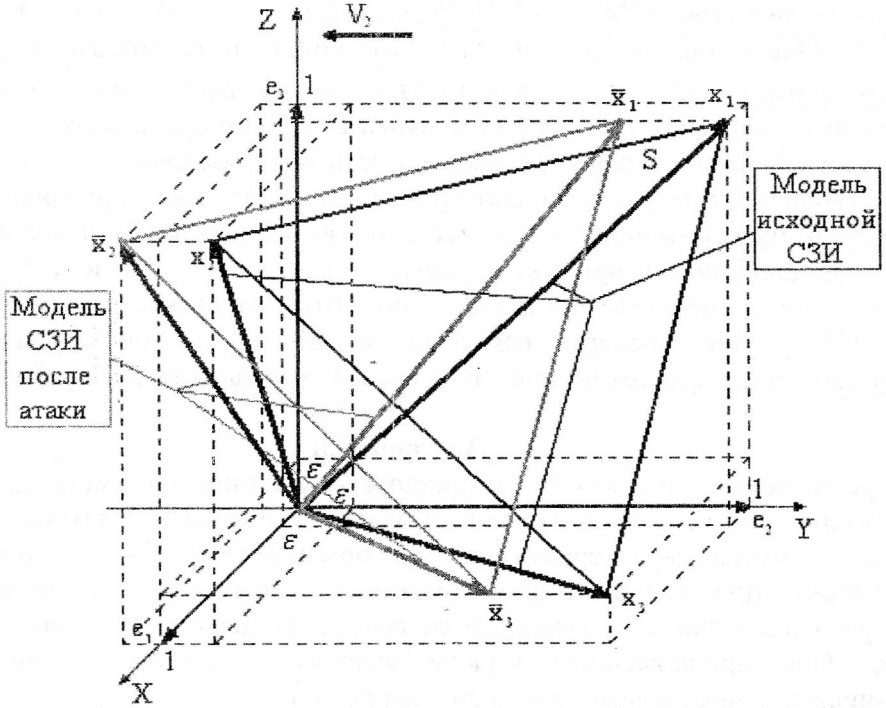

Рисунок 2. Геометрическая модель исходной СЗИ и результата проведенной атаки

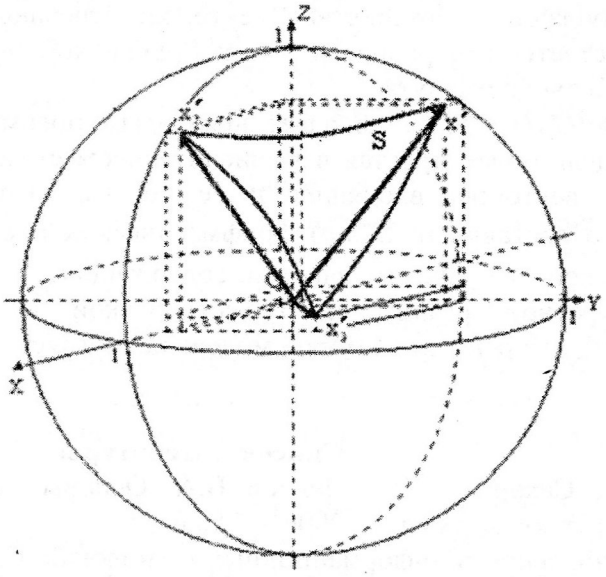

Рисунок3. Геометрическая модель СЗИ, основанная на векторной nsign-чувствительности

Замечание 2. Будем предполагать, что среди всех средств защиты, принадлежащих моделируемой СЗИ, нет таких, для которых все атаки из множества V являются опасными, т.е.

среди построенных первоначально ненормированных векторов $x_1, x_2, ..., x_m$ нет sign-чувствительного по всем координатам вектора $x_i = (\varepsilon, \varepsilon, ..., \varepsilon)^T$, поскольку его нормализация приведет к nsign-нечувствительному вектору $\left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, ..., \frac{1}{\sqrt{n}}\right)^T$, переведя соответствующее средство защиты при переходе к модели $GM2$ в другой статус: для него все атаки станут безопасными, что не будет соответствовать действительности.

Замечание 3. В качестве меры НЗЧ (n-меры) произвольного нормированного вектора $x = (x^1, x^2, ..., x^n)^T$ естественно ввести степень его отличия от n-оптимального. Для численного отражения такой меры логично использовать угол между векторами x и n-оптимальным. Поскольку определить наименее sign-чувствительный вектор не представляется возможным, то установление аналога n-меры для sign-чувствительности векторов невозможно.

Замечание 4. Введение n-меры позволяет сравнивать различные нормированные вектора с точки зрения их nsign-чувствительности к возмущающим воздействиям, а значит осуществлять выбор наименее и наиболее nsign-чувствительных векторов – имеющих наименьший и наибольший угол с n-оптимальным соответственно. Это дает возможность в геометрической модели СЗИ $GM2$ для выбора наиболее «слабого» к предполагаемым атакам, рассматриваемым во всей своей совокупности, средства защиты, а также наиболее «сильного».

4. Заключение

В работе предложены два способа построения геометрической модели СЗИ, в основу которых положены sign-, nsign-чувствительность вектора, выступающая в роли математического параметра, характеризующего информационный объект, а именно, средство защиты информации, при его векторном математическом моделировании, качественное изменение которого различно в зависимости от возмущающего воздействия, что никогда не делалось ранее. Обе предложенные модели являются наглядными, иллюстративными, простыми в вычислительном смысле при своей реализации.

При предложенном способе моделирования последствия sign-чувствительности (nsign-чувствительности) наглядно указывают на «слабые» и «сильные» звенья в СЗИ за счет разной реакции на одно возмущающее воздействие векторов, отвечающих различным средствам защиты (вектор либо остается в первоначальном координатном ортанте, либо изменяет его). Таким образом, цель работы достигнута.

Каждая из моделей $GM1$, $GM2$ обладает некоторым преимуществом по сравнению с другой. Так первая модель более простая в вычислительном смысле при реализации, т.к. не требует нормирования векторов, входящих в ее состав, вычислительные затраты для осуществления которого составляют $\underline{O}(mn)$ арифметических операций, вторая модель дает больше информации о свойствах средств защиты, содержащихся в моделируемой СЗИ. Таким образом, выбор конкретной реализации геометрической модели будет определяться непосредственно задачей, для решения которой модель используется.

Список литературы

1. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. – М.: Издательский центр «Академия». – 2006. – 256 с.
2. Домарев В.В. Безопасность информационных технологий. Системный подход. – Изд-во: ТИД «ДС». – 2004. – 992с.
3. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком. - 2004. - 280с.

5. Жданов А.А. О методе автономного адаптивного управления. Научная сессия МИФИ – 2004. VI Всероссийская научно-техническая конференция «Нейроинформатика - 2004»: Лекции по нейроинформатике. Часть 2. – М.: МИФИ, 2004. – 200 с.
6. Осовецкий Л.Г., Нестерук Г.Ф., Бормотов В.М. К вопросу иммунологии сложных информационных систем // Изв.вузов. Приборостроение. – 2003. - Т.46, №7. - С.34-40.
7. Кобозева А.А., Хорошко В.А. Модель системы защиты информации, основанная на принципах естественной системы управления // «Захист інформації». – 2007. - Спецвипуск, с.56-62.
8. Кобозева А.А., Хорошко В.А. Методика оценки адекватности системы защиты информации // Вісник ДУІКТ. – 2007. – т.5, №3. – С. 328-334.
9. Каханер Д., Моулер К., Нэш С. Численные методы и программное обеспечение. – М.: Мир, 2001. – 575 с.
10. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы.- М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.
11. Кобозева А.А. Sign-чувствительность и ее использование в стеганографических алгоритмах // Вестник Херсонского национального технического университета. - 2007. - №2(28). - С. 142-146.
12. Кобозева А.А., Борисенко И.И. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений // «Праці УНДІРТ». – 2006. - №3(47). - С. 78-83.
13. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. - 430 с.
14. Г.М. Фихтенгольц. Курс дифференциального и интегрального исчисления. – М.: Наука, 1969.

Поступила 20.03.2008г.

УДК 621.391:519.7:510.5

А. Л. Волошин

МЕТОДИКА ФОРМИРОВАНИЯ МАТРИЦ НАД КОЛЬЦАМИ ВЫЧЕТОВ ДЛЯ ПОСТРОЕНИЯ ЛИНЕЙНЫХ ПРОТОКОЛОВ МНОЖЕСТВЕННОГО РАЗДЕЛЕНИЯ СЕКРЕТА С МНОГОАДРЕСНЫМ СООБЩЕНИЕМ ДЛЯ ЗАДАННОЙ ИЕРАРХИИ ДОСТУПА

Введение

Протокол разделения секрета (ПРС) представляет собой криптографический протокол, позволяющий “разделить” некоторый секретный параметр (секрет) среди множества участников протокола таким образом, чтобы только некоторые, заранее определенные (разрешенные) коалиции участников могли восстановить его значение при объединении хранящейся у них индивидуальной секретной информации (проекций секрета). Протокол разделения секрета называется совершенным, если участники запрещенных коалиций не могут получить никакой апостериорной информации о значении секрета из имеющихся у них проекций [1].

Свойства и способы построения протоколов разделения единственного секрета интенсивно изучались, начиная с 1979 года, в [2 – 9] и ряде других работ. В силу простоты схемно-технической реализации и вычислительной эффективности особый интерес исследователей вызвали конструкции линейных ПРС, основанных на линейных (над конечными полями, кольцами вычетов и т.д.) математических преобразованиях (см., например, работы [4 – 9]).

Естественным обобщением ПРС на случай нескольких секретов являются протоколы множественного разделения секрета (ПМРС), впервые введенные в статье [10] и формально