

ПРИМЕНЕНИЕ КАЛМАНОВСКОЙ ФИЛЬТРАЦИИ К ОПРЕДЕЛЕНИЮ ДОСТОВЕРНОСТИ ЭЛЕМЕНТОВ ИНТЕГРИРОВАННОЙ БАЗЫ ДАННЫХ

2. Fridrich, J., Goljan M. Practical Steganalysis – State of the Art [текст]/J. Fridrich, M. Goljan // Proc. SPIE Photonics West . - Vol. 4675. - Electronic Imaging 2002, Security and Watermarking of Multimedia Contents. - San Jose, California. – 2002. - pp.1-13.
3. Farid, H., Siwei, L. Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines [текст]/H. Farid, L. Siwei // Information Hiding. 5-th International Workshop. Lecture Notes in Computer Science. - Vol. 2578. Springer-Verlag, - Berlin Heidelberg New York. - (2002. –pp. 340–354.
4. Avcibas, I., Memon N., Sankur B. Steganalysis using Image Quality Metrics [текст]/I. Avcibas, N. Memon, B. Sankur // SPIE Security and Watermarking of Multimedia Contents II, Electronic Imaging. - San Jose, CA. – 2001.
5. Хайкин, С. Нейронные сети: полный курс [Текст]/ С. Хайкин. – М.: Издательский дом «Вильямс», 2006. – 1106 с.
6. Jsteg [электронный ресурс]: Режим доступа: <http://jsteg.org/jstegtest.zip>.
7. F5 [электронный ресурс]: Режим доступа: <http://wwwn.inf.tudresden.de/~westfeld/attacks.html>.

Д.т.н. профессор Абденов А.Ж. тел. (383)346-08-53, abdenov@ngs.ru, Новосибирский государственный технический университет; аспирант Леонов Л.С., тел. (383)346-08-53, adanov@ngs.ru, Новосибирский государственный технический университет

УДК: 004.651.5

ПРИМЕНЕНИЕ КАЛМАНОВСКОЙ ФИЛЬТРАЦИИ К ОПРЕДЕЛЕНИЮ ДОСТОВЕРНОСТИ ЭЛЕМЕНТОВ ИНТЕГРИРОВАННОЙ БАЗЫ ДАННЫХ

Р.Н. Заркумова

В статье рассматривается понятие интегрированной базы данных как взаимосвязанной совокупности базы данных, базы знаний и базы моделей, используемых для решения задач оценки уровня безопасности информации. Для оценки качественной стороны достоверности элементов или фрагментов интегрированной базы данных использован подход калмановской фильтрации.

Ключевые слова: база данных, база знаний, база моделей, достоверность информации, фильтр Калмана

Введение.

Известно [1], что интегрированная база данных (ИБД) представляет собой взаимосвязанную совокупность собственно базы данных (БД), базы знаний (БЗ) и базы моделей (БМ). При решении задачи оценки уровня безопасности информации эксперт (или экспертная группа), опираясь на ИБД, должен разработать специфический алгоритм извлечения базы знаний и новых данных, для защиты информации интересующих пользователей и владельца информационных ресурсов.

Нетрудно видеть, что указанный алгоритм в отличие от известного алгоритма вычислительного эксперимента с имитационным моделированием Р. Шеннона [2] имеет признаки, характерные для самоорганизующихся систем, и позволяет эксперту использовать данные, знания, объективные и субъективные модели для решения поставленной проблемы в условиях неопределенности БД, неполноты БЗ и БМ. При этом из всех аспектов, связанных с созданием ИБД, решающее зна-

чение приобретает проблема достоверности входящей в нее информации.

Определим достоверность как «уровень разумной уверенности в истинности некоторого высказывания, который удовлетворяет некоторым правилам непротиворечивости и в соответствии с этими правилами формально может быть выражен числом» [3].

Известные подходы к решению проблемы оценки достоверности связаны с применением теоремы Байеса (в широком смысле) [4], теории фильтрации Калмана [5], теории нечетких множеств [6], на основе которых разработаны и применяются в экспертных системах практические способы объединения свидетельств, регистрирующих количественные, качественные и логико-семантические связи между фрагментами базы данных.

Используя идею подхода калмановской фильтрации [5], можно поставить вопрос о качественной стороне достоверности или элементов, или фрагментов, или блоков ИБД в более общем плане, чем это делалось раньше, рассматривая любой ее фрагмент как гипотезу, а фрагменты (элементы), с ко-

торыми он связан, как свидетельства относительно фрагмента-гипотезы или элемента-гипотезы. Под фрагментом ИБД будем понимать часть содержания или структуры, обладающую свойством дискретности и независимости (в идеале содержит одно независимое понятие), т.е. некоторую совокупность данных или высказываний, имеющую самостоятельный смысл.

Истинность (**И**) элемента, фрагмента, блока информации, поступающего в ИБД, зависит от объективности и достоверности источника информации и методики ее получения. Каждый вновь поступающий в ИБД новый элемент информации, фрагмент, блок знаний зависит от объективности и истинности элемента информации и его достоверности. Здесь фрагменты-свидетельства можно разбить на классы: прямые свидетельства и косвенные свидетельства информации.

Косвенные, в свою очередь, можно представлять как условные свидетельства информации (**УСИ**) и связанные свидетельства информации (**ССИ**).

Под прямыми свидетельствами будем понимать фрагменты типа измерения значения фрагмента-гипотезы. Они составляют выборку, на основании которой могут быть рассчитаны оценки значения фрагмента-гипотезы, и регистрируют, в основном, статистические связи между фрагментами.

Под условными свидетельствами информации будем понимать фрагменты типа «если (A и B), то C с достоверностью (вероятностью) P ». С их помощью можно регистрировать качественные экспертные оценки, логические связи между фрагментами и априорные знания о фрагменте-гипотезе (условные применения того или иного метода, условные функции распределения, условные плотности распределения и т.п.).

Связанные свидетельства информации регистрируют функциональные или системные связи между фрагментом-гипотезой и другими фрагментами [3], т.е. структуру некоторой автономной части ИБД (формулы, модели и т.п.).

Для описания процесса модификации (обновления) информации, знаний можно рассмотреть понятия системного значения (**СЗ**) и системной достоверности (**СД**) [2,3] фрагмента ИБД, определяемых с учетом всех свидетельств информации, знаний, моделей, содержащихся в ИБД.

Таким образом, с учетом введенной классификации проблема оценки достоверности сводится к разработке методов определения в качестве атрибутов фрагмента-

гипотезы ИБД системных достоверностей фрагментов информации, знаний, являющихся для данного фрагмента-гипотезы свидетельствами, а также системной достоверности данного фрагмента-гипотезы об информации, знаниях.

Использование методов калмановской фильтрации к определению достоверности фрагментов ИБД

Общая постановка задачи кусочно-дифференциальной квазиоптимальной фильтрации имеет следующий вид:

$$x(t_{k+1}) = A(t_{k+1}) \cdot x(t_k) + W(t_{k+1}),$$

$$x(t_0) = \bar{x}(0) = x_0, \quad (1)$$

$$y(t_{k+1}) = H(t_{k+1}) \cdot x(t_{k+1}) + V(t_{k+1}), \quad (2)$$

где (1) описывает структуру и динамику исследуемой системы, а уравнение наблюдений (2) определяет механизм образования данных, доступных для эксперта-аналитика. Здесь:

$x(t_k)$ – вектор состояния исследуемой системы;

$W(t_k)$ – случайный вектор помех исследуемой системы, связанных с погрешностями методов моделирования и экспертными характеристиками с нулевым средним и ковариационной матрицей Q ;

$A(t_k)$ – переходная матрица состояния; предполагается, что на элементарном временном промежутке процесс квазистационарный, а значит матрица $A(t_k) = A_k$, т.е. матрица постоянна;

$x(t_0)$ – вектор начального состояния с математическим ожиданием $x(0)$ и ковариационной матрицей $P(t_0) = P(0) = P_0$;

$\{y(t_k), k = 1, 2, \dots, N\}$ – последовательность векторов наблюдений;

$V(t_k)$ – случайный вектор шумов наблюдения, связанных с погрешностями канала получения информации (шумов измерительной системы) и с предполагаемыми экспертными характеристиками – с нулевым математическим ожиданием и корреляционной матрицей $R(t_l)$ постоянна, т.е. $R(t_l) = R_l, l = 1, 2, \dots, M$, где M – число временных интервалов, на котором процесс квазистационарный;

$H(t_k)$ – матрица наблюдения, которая на интервалах квазистационарности постоянна, но которая может зависеть от значений элементов переходной матрицы состояния; $H(t_k) = H(A, d_k, t_k)$;

d_k – вектор вариативности, характеризующий текущее состояние и структуру сис-

темы и канала получения информации (при этом нарушение в системе рассматривается как изменение её параметров или структуры).

Задача калмановской фильтрации [5, 7] заключается в получении по последовательности наблюдений $y(t_N) = \{y(t_1), \dots, y(t_N)\}$ оценки вектора состояния $x(t_k)$, оптимальной по критерию минимума среднего квадратического отклонения и ее корреляционной матрицы.

Допустим, эксперт располагает последовательностью $y(t_N)$ наблюдений за исследуемым объектом. На основе этих наблюдений и предшествующего опыта (априорная информация) эксперт выдвигает гипотезы A и H о структуре и параметрах наблюдаемого объекта и источника информации. Задавшись начальными условиями, он может теперь проверить справедливость своей гипотезы, последовательно применяя алгоритм фильтрации для уточнения параметров A и H с помощью каждого из имеющихся наблюдений.

Р – оценка корреляционной матрицы ошибок состояния X .

Предложенный алгоритм позволяет эксперту каждый раз при поступлении в ИБД новых данных $y(t_k)$ об исследуемом объекте рекуррентно модифицировать оценку значения его вектора состояния $x(t_k)$ и корреляционную матрицу ошибок $P(t_k)$, характеризующую достоверность этой оценки, с учетом всех поступивших на данный момент наблюдений $y(t_k)$, а также динамики и структуры изучаемого объекта и каналов получения информации.

Критерием достоверности гипотезы (A, H) здесь могут быть: расхождение k реального наблюдения $y(t_{k+1})$ и прогноза для наблюдения на k -том шаге $\hat{y}(t_{k+1} | t_k)$:

$$v(t_{k+1}) = y(t_{k+1}) - \hat{y}(t_{k+1} | t_k) = \\ = y(t_{k+1}) - H(A(t_k), d_k) \cdot \hat{y}(t_{k+1} | t_k), \quad (3)$$

а также динамика изменения корреляционной матрицы $P(t_{k+1} | t_{k+1})$ для фильтрационной оценки вектора состояния $x(t_k)$.

Если они достаточно малы, это говорит о том, что эксперт-аналитик верно идентифицировал по поступившей информации структуру и параметры объекта и источника информации. Если нет – необходимо изменить гипотезу для A или H .

С этой целью рассмотрим множество возможных структур исследуемого объекта $\{A\}$ и источника информации $\{H\}$. Пусть

таких структур μ . Тогда допустимое значение $d_i (i = 1, \dots, \mu)$ вектора d представляет одну из возможных структур исследуемого объекта и источника информации об объекте.

В общем случае d может изменяться на каждом шаге и на k -том шаге образует произвольную последовательность $D_1(k)$ из k допустимых значений вектора d . Число N_μ таких последовательностей, образующих множество $D\{D_1(k)\}$, определяется выражением:

$$N_\mu = \mu^k. \quad (4)$$

Легко видеть, что $N_\mu \rightarrow \infty$ при $\mu > 1$ и $k \rightarrow \infty$.

Для каждой последовательности $D_1(k)$, в предположении, что она осуществилась на самом деле, на основании имеющихся наблюдений может быть вычислено значение вектора состояния и его достоверность.

Из теории калмановского оценивания известно, что критерий минимума среднего квадратического отклонения приводит к оценкам условного среднего [5]:

$$\hat{x}(t_k | t_k) = E[x(t_k) | Y(t_k), D_1(k)], \quad (5)$$

а их качество определяется условной корреляционной матрицей ошибок оценивания

$$P(t_k | t_k) = E\{[x(t_k) - \hat{x}(t_k | t_k)] \times \\ \times [x(t_k) - \hat{x}(t_k | t_k)]^T | Y(t_k), D_1(k)\}. \quad (6)$$

Опуская вывод, запишем (5) и (6) в развернутом виде:

$$\hat{x}(t_k | t_k) = \sum \hat{x}_1(t_k | t_k); P[D_1(k) | Y(t_k)], \quad (7)$$

где $\hat{x}(t_k) = E[x(t_k) | Y(t_k), D_1(k)]$ – частная оценка вектора состояния $x(t_k)$, т.е. оптимальная оценка, полученная для конкретной реализации $D_1(k)$ последовательности d_k и удовлетворяющая критерию минимума среднего квадратического отклонения;

$P[D_\mu(k) | Y(t_k)]$ – апостериорная вероятность этой реализации;

$$P(t_k | t_k) = \sum_\mu \{\bar{P}_\mu(t_k) + D \cdot P_\mu(t_k)\} \times \\ \times P[D_\mu(k) | Y(t_k)], \quad (8)$$

где

$$\bar{P}_\mu(t_k) = E[\hat{x}_\mu(t_k) \times \hat{x}_\mu^T(t_k) | Y(t_k), D_\mu(k)]; \quad (9)$$

$$D \cdot P_\mu(t_k) = [\hat{x}_\mu(t_k) - \hat{x}(t_k | t_k)] \times \\ \times [\hat{x}_\mu(t_k) - \hat{x}(t_k | t_k)]^T; \quad (10)$$

μ – номера всех возможных $D_\mu(t_k)$;

$$\hat{x}_\mu(t_k) = x_\mu(t_k) - \hat{x}_\mu(t_k | t_k).$$

В этих выражениях $P_\mu(t_k)$ и $D \cdot P(t_k)$ есть соответствующие корреляционные матрицы ошибок частных оценок вектора состояния.

Таким образом, в общем виде алгоритм оптимальной фильтрации представляет следующую последовательность вычислений:

- для принятой реализации наблюдения $Y(t_k)$, на элементарном временном интервале, рассчитываются частные оценки вектора состояния для всех возможных реализаций $D_\mu(k)$ и соответствующие частные корреляционные матрицы;

- далее рассчитываются значения $P[D_\mu(k) | Y(t_k)]$, играющие роль весовых коэффициентов в уравнениях (7) и (8);

- рассчитывается по (7) оптимальная оценка вектора состояния $x(t_k)$;

- рассчитывается по (8) корреляционная матрица ошибок оценивания;

- рассчитывается прогноз оценки, ее корреляционной матрицы и наблюдения на следующий шаг;

- рассчитываются переходная матрица исследуемой системы, матрица канала наблюдения и корреляционные матрицы шумов на следующий шаг [5].

Это процесс сходится при достаточно общих предположениях (если угаданы структура и опорные матрицы состояния и наблюдения), причем особенно эффективно уточнение параметров идет на основе процедур активной идентификации [7], а также во время первых нескольких шагов.

При практической реализации алгоритма оптимальной фильтрации возникают следующие проблемы:

- при возрастании числа наблюдений k на интервале квазистационарности неограниченно возрастает число итераций и, следовательно, число частных оценок, что требует неограниченных вычислительных ресурсов;

- требуется разработка конкретных подходов к вычислению частных оценок вектора состояния, соответствующих стартовых корреляционных матриц, вероятности различных последовательностей $D_\mu(k)$, а также различные характеристики шумовых процессов и других стартовых оценок.

Возможные пути преодоления этих трудностей могут быть сведены к следующему:

- выбор определенных структур для исследуемой системы и канала наблюдения, в частности, рекомендуется начинать подби-

рать структуры уравнений как можно упрощенными;

- выбор определенных классов $d(t_k)$ и $D_\mu(k)$;

- ограничение числа учитываемых наблюдений;

- введение некоторых гипотез при аппроксимации прогноза значения вектора состояния исследуемой системы.

В итоге задача может решаться в следующей постановке:

$$x(t_{k+1}) = d_1(t_k) \cdot A(t_{k+1}, t_k) \cdot x(t_k) + d_2(t_k) \cdot w(t_k), \quad (11)$$

$$y(t_{k+1}) = d_3(t_{k+1}) \cdot H(A, t_{k+1}) + d_4(t_{k+1}) \cdot v(t_{k+1}), \quad (12)$$

где сделаны следующие предположения:

- структура исследуемой системы и канала наблюдения на элементарном временном интервале линейна и квазистационарна;

- шумы $w(t_k)$ и $v(t_k)$ – белые, гауссовские и некоррелированы между собой и с вектором $x(t_k)$.

В уравнениях (11) и (12) $d(t_k) = \{d_1(t_k), d_2(t_k), d_3(t_k), d_4(t_k)\}$ задают конкретные возможные режимы исследуемой системы и канала наблюдения, например:

$d(t_k) = \{1, 1, 1, 1\}$ – нормальный режим функционирования исследуемой системы и канала наблюдений, когда эксперту известны с точностью до шумов их структура и параметры;

$d(t_k) = \{1, 1, 1, k+1\}$ – в канале наблюдения резко возрос уровень шума, в результате чего возрос разброс поступающих к эксперту данных без изменения среднего значения вектора состояния исследуемой системы;

$d(t_k) = \{1, 1, 0, 1\}$ – отсутствует информация в канале наблюдения, в результате чего в поступающих к эксперту данных пропала систематика, и остался один белый шум;

$d(t_k) = \{1, 1, 1, s+1\}$ – отсутствует информация в канале наблюдения, и в тоже время резко возрос шум; такой вариант означает, скорее всего, что изменилось содержание поступающей информации, а эксперт, не умея «расшифровать» эту информацию, принимает ее за шум;

$d_1(t_k) = \{1, 0, 1, 1\}$ – отсутствуют шумы в модели исследуемой системы, т.е. эксперт-аналитик сумел подобрать относительно точную детерминированную модель;

$d(t_k) = \{1, s+1, 1, 1\}$ – резко возросли шумы в модели исследуемой системы; при этом если шум остался белым, то модель эксперта верна, но сам исследуемый объект стал ме-

нее детерминированным, а если шум окрашен (имеет систематику), то модель эксперта-аналитика требует уточнения (систематические ошибки должны быть расшифрованы экспертом и включены в модель исследуемой системы).

Таким образом, видно, что даже с приведенным сравнительно простым набором возможных значений вектора вариативности $d(t_k)$ можно описать широкий круг проблем, связанных с достоверностью фрагмента ИБД, а в более широком плане – получить универсальный и гибкий формальный аппарат модификации фрагментов ИБД при поступлении в нее нового фрагмента.

Исследование конкретной проблемы, стоящей перед экспертом, следует начинать с тех случаев, когда изменения и модификации затрагивают прежде всего канал наблюдения. Если эксперт изучает некоторую сложную систему (объект) достаточно долго, то имеет определенное представление о ее структуре и параметрах, пусть и не очень точное. В этой ситуации главной становится оценка достоверности источников информации, а задача уточнения параметров исследуемой системы решается по мере решения первой задачи. Для такой постановки $d(t_k) = \{1, 1, d_3(t_k), d_4(t_k)\}$ и соответственно, система уравнений принимает вид:

$$x(t_{k+1}) = A(t_{k+1}, t_k) \cdot x(t_k) + w(t_k), \quad (13)$$

$$y(t_{k+1}) = d_3(t_{k+1}) \cdot H(t_{k+1}, A) + d_4(t_k) \cdot v(t_k), \quad (14)$$

Для нормального режима функционирования исследуемой системы и канала наблюдения уравнение имеет вид:

$$x(t_{k+1}) = A(t_{k+1}, t_k) \cdot x(t_k) + w(t_k), \quad (15)$$

$$y(t_{k+1}) = H(t_{k+1}) \cdot x(t_{k+1}) + v(t_{k+1}), \quad (16)$$

а алгоритм модификации вектора состояния исследуемой системы для k -того элементарного временного интервала есть классический калмановский алгоритм оптимального фильтра [5].

Q , R – корреляционные матрицы шумов системы и канала наблюдений;

$P(t_0)$ – корреляционная матрица начального стартового состояния исследуемой системы.

Располагая этим алгоритмом, можно досконально изучить на этапе предварительного моделирования исследуемую систему, основной режим работы которой описывается линейной системой уравнений, а также получить все частные оптимальные оценки вектора состояния системы и их корреляционные матрицы, что снимает часть перечисленных

выше проблем реализации общего алгоритма оптимальной фильтрации.

Наибольшие трудности вызывает корректное вычисление условной вероятности $p[D_\mu(k) | Y(t_k)]$ даже для несложных систем.

Анализ точных выражений для $p[D_\mu(k) | Y(t_k)]$ показывает, что для многих случаев, связанных с исследованием уровня безопасности информации, данную вероятность можно аппроксимировать двумя-тремя значениями типа $0 - \frac{1}{2} - 1$ (нет - может быть - да).

Дело в том, что особенностью экспертных задач оценки уровня безопасности информации является, как отмечалось выше, неполнота данных, которыми располагает эксперт практически на всех этапах исследования сложного объекта. Принцип баланса точности рекомендует в таких случаях не пользоваться тонкими сложными методами моделирования, поскольку их точность будет загружена неполнотой и неточностью исходной информации, а их сложность практически неизбежно приведет к некорректному результату в силу неадекватности отдельных частей модели и объекта. В соответствии с этим принципом должен соблюдаться некоторый разумный баланс между требующейся точностью ответа, точностью исходных данных, точностью модели и точностью метода исследования. В этом смысле сделанное допущение вполне разумно, особенно на первых этапах исследования сложного объекта, когда проверяются, в основном, правильность структуры исследуемой системы и канала наблюдения, а также области возможных значений их параметров. Критерием здесь может быть отклонение очередного наблюдения от его прогноза, например:

$$P[D_\mu(k) | Y(t_k)] = \begin{cases} 0, & \text{если } |z| > r_0 \cdot \sqrt{\det P_z}, \\ 1, & \text{если } |z| > r_1 \cdot \sqrt{\det P_z}, \\ 0 < r_1 < r_0, \\ 1/2 & \text{в иных случаях,} \end{cases}$$

т.е. вычисление условной вероятности предельно упрощается: необходимо только сравнить поступившее наблюдение $y(t_k)$ с некоторыми пороговыми значениями и выбрать соответствующее значение $p[D_\mu(k) | Y(t_k)]$.

Вывод.

В данной работе было дано понятие интегрированной базы данных как взаимосвя-

РАЗДЕЛ V. СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

занной структуры базы данных, базы знаний, базы моделей. Для повышения уровня достоверности элементов интегрированной базы данных предложено использование аппарата фильтра Калмана.

СПИСОК ЛИТЕРАТУРЫ

1. Элти, Дж. Экспертные системы: концепции и примеры./ Дж. Элти, М.Кумбс. – М.: Финансы и статистика, 1987.
2. Шумский, А.А. Системный анализ в защите информации. / А.А. Шумский, А.А. Шелупанов.– М.: Гелиос АРВ, 2005. – 224с.
3. Перегудов, Ф.И. Введение в системный анализ./ Ф.И. Перегудов, Ф.И. Тарасенко. – М.: Высшая школа, 1989.
4. Зельнер, А. Байесовские методы в эконометрии./ А. Зельнер – М.: Статистика, 1980.
5. Браммер, К., Зиффлинг Г. Фильтр Калмана-Бьюси. / К. Браммер, Г. Зиффлинг.– М.: Наука, 1982.
6. Zadeh, L. Fuzzy sets/ L. Zadeh // Information and Control. – 1965. - №8.
7. Абденов, А.Ж. Активная идентификация стохастических непрерывно-дискретных динамических систем на основе спектральной плотности мощности входного сигнала/ А.Ж. Абденов// Автометрия. – 1999. - №1. – С. 74-93.

Аспирант **Заркумова Р.Н.**, тел. (383)346-08-53, zarkumova@gmail.com, Новосибирский государственный технический университет.