ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2014. Т. 18, № 3 (64). С. 270–275 http://journal.ugatu.ac.ru

УДК 004.056

МЕТОДИКА ФОРМИРОВАНИЯ И ПОПОЛНЕНИЯ БАЗИСА ТИПОВЫХ СИТУАЦИЙ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. А. ДУЛЕНКО[1], В. А. ПЕСТРИКОВ[2], К. В. КУРОЧКИНА[3]

[1] dulenko@rambler.ru, [2] vpestrik@mail.ru, [3] ray_of_sun91@mail.ru

ФГБОУ ВПО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 8 апреля 2014 г.

Аннотация. Рассматривается методика формирования и пополнения базиса типовых ситуаций систем поддержки принятия решений по обеспечению информационной безопасности, основанной на принципе отделимости. Предложено отнесение текущей ситуации к одному из типовых классов на основе нечеткого отношения сходства между ними. Показано, что классификация ситуаций по сходству представляет собой математическое разложение вектора признаков по некоторому базису признакового пространства. Предложена алгебраическая процедура разложения векторов-признаков для сходных ситуаций, обеспечивающая наилучшее приближение к эталонным наборам в смысле наименьших квадратов отклонений. Предложенная методика формирования и пополнения базиса типовых ситуаций позволит эффективно осуществлять анализ решений и усваивать опыт ЛПР по принятию решений.

Ключевые слова: информационная безопасность; система поддержки принятия решений; лицо, принимающее решения; базис типовых ситуаций; разделяющая гиперплоскость; эталонный вектор.

ВВЕДЕНИЕ

В современных промышленных предприятиях производственные и бизнес-технологии непосредственным образом интегрированы в общую ИТ-инфраструктуру, степень развития которой влияет на эффективность функционирования предприятия. Однако с ростом значимости, увеличением сложности и глобализацией информационных технологий резко возрастает и значимость проблемы защиты информационных и интеллектуальных ресурсов предприятий. Это делает вопросы обеспечения информационной безопасности чрезвычайно актуальными.

С целью предотвращения инцидентов информационной безопасности на средних и крупных предприятиях создаются службы информационной безопасности, в задачи которых входит выявление, локализация и устранение угроз информационной безопасности.

В связи с необходимостью принятия решений в условиях ограничений по времени и другими ресурсами, возрастает вероятность принятия ошибочных решений, которые могут повлечь финансовые убытки, а также потерю информации, содержащей коммерческую тайну, необходимой для более эффективного функционирования предприятия.

Одним из направлений повышения эффективности действий при обнаружении угроз информационной безопасности является разработка и внедрение систем поддержки принятия решений (СППР) [1]. Ключевым элементом в таких СППР является базис типовых ситуаций и соответствующих им типовых решений. Существующие методики формирования такого базиса [1–4] отличаются сложностью и требуют затрат значительных вычислительных ресурсов.

ПРЕДЛАГАЕМЫЙ ПОДХОД К РАЗРАБОТКЕ МЕТОДИКИ

Предлагаемая методика может быть реализована в системах поддержки принятия решений и пригодна для подготовки и принятия решений как в условиях, когда ситуация является не новой, так и в случае, когда ситуация появляется впервые. Наличие признаков типовой ситуации позволяет СППР работать в автоматическом режиме и выдавать лицу, принимающему решения (ЛПР), рекомендации о возможных типовых решениях. Для обеспечения этого режима в системе необходимы решающие правила или алго-

ритмические процедуры отнесения текущей ситуации к одному из типовых классов.

Другая функция СППР связана с первым появлением ситуации и должна обеспечивать включение новой ситуации в список базисных, в которых информация о признаках и действиях пополняется на основе успешных действий ЛПР. Ниже приводятся методики, предлагаемые для решения этих задач.

Построение решающих правил, позволяющих отнести текущую ситуацию к одному из выбранных классов, предлагается проводить на основе нечеткого отношения сходства между ситуациями. При этом очевидно, что мера сходства μ_s является величиной положительной, значения которой лежат между 0 и 1.

Исходя из этих посылок, задача классификации ситуаций по сходству представляет собой математически разложение вектора признаков ситуации по некоторому базису признакового пространства. При этом базис должен быть выбран таким, чтобы все коэффициенты разложения были бы положительными.

Инциденты, связанные с нарушением целостности системы информационной безопасности, как правило, не документируются и не афишируются в прессе, поэтому их типовой набор весьма ограничен и не является полным. В этих условиях в системе должна быть предусмотрена процедура расширения базиса как следствие накопления опыта по ликвидации нештатных ситуаций. Такая процедура базируется на теории решения систем линейных неравенств и, в частности, на теореме о разделяющей гиперплоскости [5]. Согласно этой теореме система $Ax = b$ либо имеет неотрицательное решение (при неотрицательных a_{ij}), если вектор b лежит внутри гиперконуса, образованного векторами-столбцами матрицы A, либо существует гиперплоскость P такая, что конус векторов-столбцов и вектор b лежат по разные стороны от нее (см. рис. 1).

На рис. 1 случай *а* соответствует возможности представления произвольного вектора b как линейной комбинации базисных векторов, имеющих положительные меры сходства с данным вектором. Случай *б* соответствует отсутствию сходства хотя бы с одним из базисных векторов ситуации.

Формальным признаком существования разделяющей гиперплоскости является наличие отрицательных коэффициентов в разложении текущего вектора ситуации в базисе векторов-столбцов матрицы A [5]. При выполнении этого условия такая ситуация должна пополнить базисный набор типовых ситуаций как не сводимая по сходству к комбинации исходных.

Предлагаемая в данной работе методика пополнения базы данных сведениями о новых ситуациях и решающие правила для оценки состояния оперативной обстановки приводится далее.

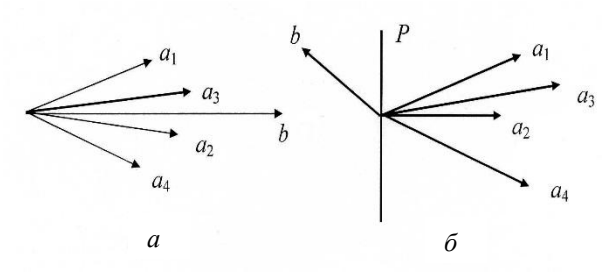

Рис. 1. Геометрическое представление классификации ситуации

На первом этапе алгоритма строится эталонный набор векторов-ситуаций $S^э_i$ (i=1,…,m) с компонентами-признаками $x^э_j$ (j=1,…,n), который образует в общем случае прямоугольную матрицу D размером $n\times m$, где n – общее количество рассматриваемых признаков ситуаций, m – начальное количество эталонных векторов ситуаций.

В общем случае матрица D имеет вид

$$D=\begin{bmatrix} x^э_{11} & x^э_{12} & \cdots & x^э_{1m} \\ x^э_{21} & x^э_{22} & \cdots & x^э_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ x^э_{n,1} & x^э_{n,2} & \cdots & x^э_{n,m} \end{bmatrix} = \begin{bmatrix} S^э_1 & S^э_2 & \cdots & S^э_m \end{bmatrix}.$$

Затем матрица эталонов (типовых ситуаций старого базиса) используется для упрощения анализа и уменьшения размерности признакового пространства путем отображения векторов-признаков размерности n- в m-мерное пространство коэффициентов разложения этих векторов-признаков в базисе эталонных векторов. Таким образом, согласно предложенной методике, для произвольного вектора признаков $S_j = \{x_j\}$ могут быть определены его коэффициенты разложения в базисе эталонных векторов. Для этого определяется вектор коэффициентов разложения B по формуле:

$$B_j=(D^TD)^{-1}D^TS_i\,, \qquad (1)$$

которая дает наилучшее (в смысле минимума квадратов отклонений) приближение S_i к наборам эталонных векторов $S^э_i$. Если окажется, что хотя бы один компонент вектора B отрицателен, то это означает отсутствие сходства между данной ситуацией и соответствующей базисной, т.е. согласно предложенному принципу она

не принадлежит к типу ситуаций, сходных с первоначально выбранными, и должна пополнить базис. Это означает, что данная ситуация встретилась ЛПР впервые, в системе отсутствуют какие-либо рекомендации о вариантах решения в ней, и ЛПР необходимо сгенерировать и разработать решения самостоятельно. В случае успешного решения информация заносится в СППР и после этого ситуация считается типизированной. Данная процедура позволяет накапливать опыт по ликвидации нестандартных экстремальных ситуаций.

Если отрицательных коэффициентов нет (текущая ситуация сходна с имеющимися в начальном наборе типовых), то отнесение к тому или иному классу предлагается производить на основании вычисления расстояния в *n*-мерном пространстве между текущей ситуацией и базисными.

Это расстояние может быть определено с использованием евклидовой метрики

$$d_E^i = \sqrt{\sum_j (b_j^Э - b_j)^2}, \qquad (2)$$

где $b^Э_j$ – коэффициенты разложения матрицы эталонных векторов.

В результате такой оценки предварительный вывод о состоянии системы информационной безопасности делается на основе значения ближайшего эталонного вектора. То есть отыскивается минимальное расстояние, соответствующее эталонному вектору $S^Э_i$:

$$\min_i \{d_E^i\} \Rightarrow S_i^Э. \qquad (3)$$

Геометрическая интерпретация предложенного метода приведена на рис. 2.

Для повышения достоверности оценки предлагается второй этап обобщенного алгоритма. На этом этапе оценивают значения решающих признаков, в качестве которых используются признаки эталона, не вошедшие в исходный набор признаков. Для этого в СППР предусматривается процедура специальных наблюдений (решающего эксперимента), а также процедура фиксации дополнительных признаков [5]. По результатам сбора этой информации при наличии данных решающего эксперимента принимается гипотеза о принадлежности к заданному классу ситуаций, либо при появлении дополнительных признаков происходит уточнение исходной ситуации (переход к первому этапу).

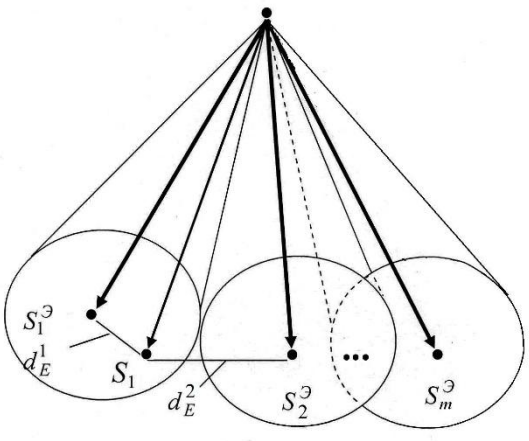

Рис. 2. Геометрическая интерпретация оценки ситуации

Обобщенный алгоритм реализации процедуры классификации ситуаций и пополнения базиса представлены на рис. 3.

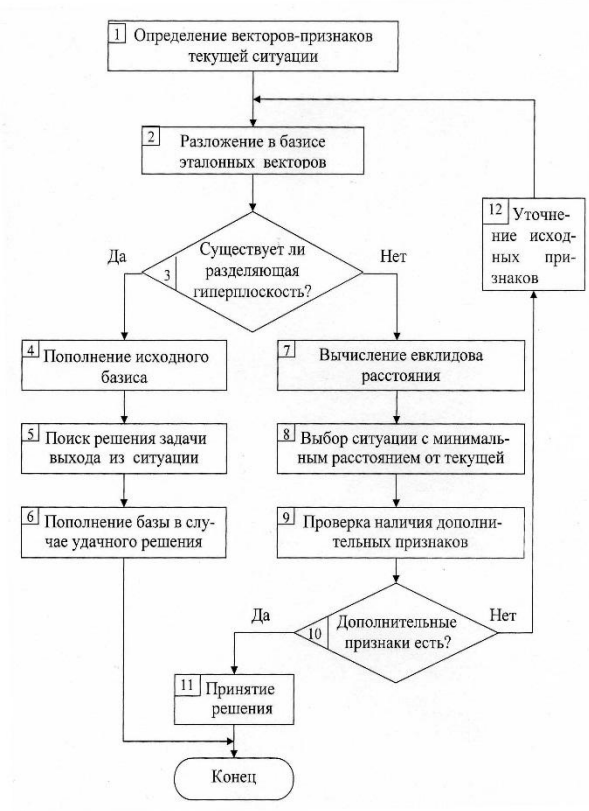

Рис. 3. Обобщенный алгоритм реализации процедуры классификации ситуаций и пополнение базиса типовых ситуаций

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА ПРЕДЛОЖЕННОЙ МЕТОДИКИ

Для проверки предложенной методики был проведен эксперимент [4, 5]. Для этого была составлена анкета, в которой необходимо было оценить по шкале 0–9 степень характерности (выраженности) признаков нарушения целост-

ности системы информационной безопасности, характеризующих одну из ситуаций: нормальная ($S_1^Э$), потенциальной уязвимости ($S_2^Э$), явной уязвимости ($S_3^Э$). Согласно используемой шкале значение «0» присваивается признаку, если он не характерен для данной ситуации, а значение «9» – максимально выраженному признаку.

Под нормальной ситуацией понимается состояние системы, при котором система обеспечения информационной безопасности работает в штатном режиме согласно заданным требованиям политик безопасности. Ситуация потенциальной уязвимости характеризуется наличием угроз в системе обеспечения информационной безопасности, реализация которых возможна только при участии сотрудников. Для ситуации явной уязвимости характерно наличие угроз в системе обеспечения информационной безопасности, для реализации которых не требуется участие персонала.

Анкетирование позволило определить итоговый перечень признаков ситуаций X:

x_1 – корректное прохождение процедуры аутентификации/идентификации;

x_2 – использование учтенных носителей;

x_3 – использование компьютера только в рабочее время;

x_4 – технологии контроля печати не выявляют аномальных отклонений;

x_5 – отсутствуют попытки нарушения дискреционного разграничения доступа;

x_6 – отсутствуют попытки нарушения мандатного разграничения доступа;

x_7 – технологии контроля трафика не выявляют аномальных отклонений;

x_8 – целостность файловой системы (ФС) обеспечена;

x_9 – целостность конфигурации персонального компьютера (ПК) обеспечена;

x_{10} – целостность конфигурации ПК не обеспечена;

x_{11} – подключение посторонних носителей к портам ПК;

x_{12} – использование компьютера в нерабочее время;

x_{13} – зафиксированы попытки нарушения дискреционного разграничения доступа;

x_{14} – зафиксированы попытки нарушения мандатного разграничения доступа;

x_{15} – целостность ФС не обеспечена;

x_{16} – нештатная работа антивируса;

x_{17} – нештатная работа межсетевого экрана;

x_{18} – зафиксирован некорректный ввод идентификационных данных перед успешной аутентификацией/идентификацией;

x_{19} – технологии контроля печати выявили нештатную ситуацию;

x_{20} – технологии контроля трафика выявили нештатную ситуацию;

x_{21} – некорректный ввод идентификационных данных;

x_{22} – попытка повышения уровня доступа пользователем;

x_{23} – попытка отключения антивирусной системы пользователем;

x_{24} – попытка отключения межсетевого экрана пользователем;

x_{25} – попытка внесения изменений в конфигурацию локальной сети и доступа к глобальной сети.

По результатам обработки анкет были сформированы векторы-признаки эталонных ситуаций $S_i^Э$ (см. табл. 1).

Таблица 1

Векторы-признаки эталонных ситуаций

X	$S_1^Э$	$S_2^Э$	$S_3^Э$
x_1	9	0	0
x_2	8	0	0
x_3	7	0	0
x_4	5	0	0
x_5	8	0	0
x_6	9	0	0
x_7	7	0	0
x_8	8	0	0
x_9	6	0	0
x_{10}	0	6	1
x_{11}	0	8	2
x_{12}	0	8	2
x_{13}	0	9	3
x_{14}	0	9	3
x_{15}	0	8	2
x_{16}	0	7	2
x_{17}	0	7	2
x_{18}	0	8	3
x_{19}	0	9	3
x_{20}	0	9	3
x_{21}	0	2	9
x_{22}	0	3	9
x_{23}	0	2	8
x_{24}	0	2	8
x_{25}	0	3	8

Преобразовав полученную матрицу по формуле (1), получили значения эталонных коэффициентов разложения $B_j^Э$ (см. табл. 2).

Для проверки правильности отнесения новой ситуации к одной из базисных в соответствии с предложенной методикой было сформировано 3 новых произвольных вектора с признаками ситуаций нарушения состояния системы информационной безопасности (см. табл. 3).

Таблица 2

Эталонные коэффициенты разложения

$B_1^Э$	$B_2^Э$	$B_3^Э$
1	0	0
0	1	$-6{,}93889*10^{-17}$
0	$-1{,}11022*10^{-16}$	1

Таблица 3

Векторы-признаки новых ситуаций

	S_1	S_2	S_3
x_1	1	0	1
x_2	1	0	2
x_3	1	0	2
x_4	3	0	3
x_5	2	0	2
x_6	1	0	2
x_7	1	0	3
x_8	0	0	2
x_9	1	0	5
x_{10}	5	1	6
x_{11}	4	1	6
x_{12}	6	2	8
x_{13}	7	2	8
x_{14}	7	1	6
x_{15}	8	2	8
x_{16}	6	2	5
x_{17}	6	3	9
x_{18}	7	4	8
x_{19}	7	6	2
x_{20}	7	1	1
x_{21}	2	5	1
x_{22}	2	7	1
x_{23}	3	7	1
x_{24}	3	9	2
x_{25}	2	9	2

Таблица 4

Результаты вычисления компонент вектора B_j

	S_1	S_2	S_3
B_1	0,150097	0	0,302144
B_2	0,771049	0,02905	0,759724
B_3	0,064571	0,861546	-0,06741

У каждого из векторов B_j нет отрицательных компонентов, значит, выбранные ситуации сходны с имеющимися в начальном типовом (эталонном) наборе.

Для новых векторов вычислены коэффициенты разложения B_j по формуле (1), расстояния между текущей ситуацией и базисной с использованием евклидовой метрики по формуле (2) и определены, к какой из базисных ситуаций относятся данные векторы. Результаты, полученные при вычислениях по формуле (1), приведены в табл. 4, по формуле (2) – в табл. 5.

Таблица 5

Результаты вычисления расстояний между текущей и базисной ситуацией

	S_1	S_2	S_3
$d^1{}_E$	1,149356	1,320267	1,033793
$d^2{}_E$	0,281278	1,298078	0,391878
$d^3{}_E$	1,221505	0,141469	1,34456

Выбирая минимальное расстояние для каждой ситуации из табл. 5, можно сделать вывод, что векторы S_1 и S_3 соответствуют эталонному вектору $S_2^Э$, а вектор S_2 – вектору $S_3^Э$.

На основе данной методики был разработан программный модуль, который можно интегрировать в действующую систему поддержки принятия решений.

ЗАКЛЮЧЕНИЕ

Таким образом, предложено пополнять базисный набор эталонных ситуаций, действия в которых достаточно хорошо отработаны. Новым элементом при этом является использование меры сходства как положительного коэффициента разложения вектора по заданному базису, существование которого определяется теоремой о разделяющей гиперплоскости. Предлагается также двухэтапная итерационная процедура оценки состояния оперативной обстановки. Предложенная методика формирования и пополнения базиса (набора) типовых ситуаций, основанная на принципе отделимости, позволит эффективно осуществлять анализ решений и усваивать опыт ЛПР по принятию решений.

Отнесение текущей ситуации к одному из типовых классов позволит на основе нечеткого отношения находить сходства между ними. Следовательно, классификация ситуаций по сходству математически представляет собой разложение вектора признаков ситуации по некоторому базису признакового пространства. При этом базис должен быть выбран таким, чтобы все коэффициенты разложения были бы положительными.

Наличие разделяющей гиперплоскости между вектором текущей ситуации и набором типовых ситуаций свидетельствует об отсутствии указанного сходства и о том, что текущая ситуация не является типовой.

СПИСОК ЛИТЕРАТУРЫ

1. **Васильев В. И., Красько А. С., Пестриков В. А.** Вопросы создания системы поддержки принятия решений в рамках программы «Безопасный город» // Вестник УГАТУ. 2008. Т. 10, № 2 (27). С. 191–199. [V. I. Vasilyev, V. A Pestrikov, and A. S. Krasko, “The questions of making decisions

support systems creation in the framework of the program 'Safe city'," (in Russian), *Vestnik UGATU*, vol. 10, no. 2 (27), pp. 191-199, 2008. **]**

2. **Бакусов Л. М.** Структурный подход к построению декомпозиции и установлению зависимостей // Управление в сложных системах: межвуз. науч. сб. Уфа: УГАТУ, 1999. С. 56-61. **[** L. M. Bakusov. "Structural Method of Decomposition Constructing Dependency Making," in *Management in Complex Systems,* (Interuniversity scientific collection), 1999, pp. 56-61, Ufa: USATU. **]**

3. **Дуленко В. А., Пестриков В. А.** Процедура принятия решений в экстремальных ситуациях на основе принципов ситуационного управления // Вестник ВЭГУ. 2013. № 5. С. 15–20. **[** V. A. Dulenko, V. A. Pestrikov. "Procedure of Decision Making in Extreme Situations Based on the Principles of Situation Control," *VEGU Bulletin*, no.5, pp. 15-20, 2013. **]**

4. **Дуленко В. А., Пестриков В. А.** Безопасный город. Классификация нештатных ситуаций, возникающих на городских территориальных объектах // Наука и образование в жизни современного общества: сб. науч. тр. по матер. Междунар. заочн. науч.-практ. конф. (Тамбов, 29 окт. 2012). Тамбов: Изд-во ТРОО «Бизнес-Наука-общество», 2012. Ч. 3. С. 43-44. **[** V. A. Dulenko, V. A. Pestrikov. "Safe City. Classification of Emergency Situations at Urban Area Facilities," in *Science and Education in Modern Society Life: science collection based on the International absentee workshop 29 October, 2012*, pp. 43-44. Tambov: Publishing House TROO Biznes-Nauka-Obchestvo, 2012. **]**

5. **Стренг Г.** Линейная алгебра и ее применения: Пер. с англ. М.: Мир, 1980. 454 с. **[** G. Strang. *Linear Algebra and Its Applications*, (Translated from English). Moscow: Mir, 1980. **]**

6. **Дуленко В. А.** Методика определения минимальной численности экспертов при проведении экспертного опроса // Вопросы образования и науки: теоретический и методический аспекты: сборник научных трудов по материалам Международной заочной научно-практической конференции (Тамбов, 30 апр. 2012). Тамбов: Изд-во ТРОО «Бизнес-Наука-общество», 2012. Ч. 2. С. 60–62. **[** V. A. Dulenko, "Methodology of Determination of the Minimal Quantity of Experts during an Expert Survey," in *Problems of Science and Education: theory and practice: science collection based on the International absentee workshop 30 April, 2012*, vol. 2, pp. 60-62, Tambov Publishing House TROO Biznes-Nauka-Obchestvo, 2012. **]**

ОБ АВТОРАХ

ДУЛЕНКО Вячеслав Алексеевич, доц. каф. выч. техники и защиты информации. Дипл. инж.-элект. (УГАТУ, 1986). Канд. техн. наук по упр. в техн. системах (УГАТУ, 1999). Иссл. в обл. сит. управления и информ. безопасности.

ПЕСТРИКОВ Владимир Анатольевич, доц. каф. выч. техники и защиты информации. Дипл. инж.-э/мех. (УГАТУ, 1983). Канд. техн. наук по упр. в техн. системах (Акад. МВД, 1996). Иссл. в обл. управления и правового обеспечения инф. безопасности.

КУРОЧКИНА Кристина Владимировна, студ. каф. выч. техники и защиты информации.

METADATA

Title: The methodology of formation and replenishment of typical situations basis in systems of decision making support on ensuring information security.

Authors: V. A. Dulenko, V. A. Pestrikov, K. V. Kurochkina.

Affiliation:
Ufa State Aviation Technical University (USATU), Russia.

Email: dulenko@rambler.ru, vpestrik@mail.ru, ray_of_sun91@mail.ru

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 18, no. 3 (64), pp. 270-275, 2014. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: The presented article concerns the methodology of forming the standard situation basis in decision support system to provide information security based on the principle of separability. It is suggested to relate the present situation to one of the typical classes on the basis of uncertain close relationship between them. It is stated that the classification of situations on the principle of close represents a mathematical resolution of feature vector on some feature space basis. It is suggested to use algebraic procedure of feature vector resolution for similar situations providing a better approximation to the reference sets in the sense of the least square deviation. The suggested methodology of forming and replenishment of the typical situation basis will help to effectively fulfill decision analysis and learn decision-maker's experience.

Key words: information security; decision support system; decision-maker; typical situations basis; separating hyperplane; reference standard vector.

About authors:

DULENKO, Vjacheslav Alexeevich, Associate professor of the Computer engineering and information security department. Certified electrical engineer (USATU, 1986). PhD in Technical Sciences: Control in engineering systems (USATU, 1999). Scientific specialization: research in the field of situation control and information security.

PESTRIKOV, Vladimir Anatoljevich, Associate professor of the Computer engineering and information security department. Certified electrical engineer (USATU, 1983). PhD in Technical Sciences: Control in engineering systems (Academy of Ministry of Internal Affairs of Russia, 1996). Scientific specialization: research in the field of management and law maintenance of information security.

KUROCHKINA, Kristina Vladimirovna, student of the Computer engineering and information security department. Scientific specialization: research in the field of information security management.