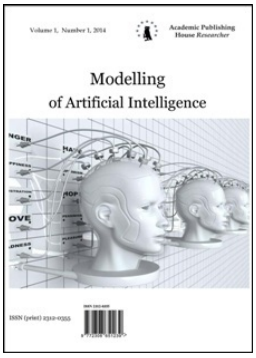
Published in the Russian Federation
Modeling of Artificial Intelligence
Has been issued since 2014.
ISSN: 2312-0355
E-ISSN: 2413-7200
Vol. 12, Is. 4, pp. 187-193, 2016

DOI: 10.13187/mai.2016.12.187
www.ejournal11.com



UDC 681.3

Enhancing Operational Efficiency of the Fuzzy Image of the Attacker's Method of Iterations

Simon Zh. Simavoryan [a, *], Arsen R. Simonyan [a], Elena I. Ulitina [a], Viktor I. Samarin [a], Rafik A. Simonyan [b], Margarita A. Kardashyan [a]

[a] Sochi State University, Russian Federation
[b] Kuban State University, Russian Federation

Abstract

The work is devoted to the development of methods to search for a fuzzy image of the attacker based on the use of the method of iterations. The search is performed on the data from the specialized knowledge base of malicious actions (patterns) and knowledge of standard situations and values of their allowable performance.

Keywords: fuzzy image of attacker, method of iterations.

1. Введение

Задача эффективного поиска нечеткого образа злоумышленника является неотъемлемой частью интеллектуальной деятельности службы защиты информации (Симаворян, 2014; Simavoryan, 2014). Поиск может быть осуществлен с помощью применения методов первоначального поиска, например, методов (процедур) итераций (Панюкова, 2013; Ченцов, 2016). Для эффективного применения методов итераций необходимо иметь достаточную информативную базу данных о злоумышленных действиях. Такая база данных может быть создана на базе следующих баз знаний: 1) специализированной базы знаний о злоумышленных действиях, элементы которой называются шаблонами; и 2) специализированной базы знаний о штатных ситуациях и допустимых их характеристиках. Метод итерации (метод последовательных приближений) – приближенный метод решения математических задач, заключающийся в построении последовательности, члены которой получаются с помощью повторного применения некоторой операции, алгоритма (Панюкова, 2013). Суть такого метода заключается в нахождении по приближённому значению величины следующего приближения (являющегося более точным).

* Corresponding author
E-mail addresses: simsim58@mail.ru (S.Zh. Simavoryan), oppm@mail.ru (A.R. Simonyan), elenaulitina@mail.ru (E. I. Ulitina), visamarin@mail.ru (V.I. Samarin), raf55@list.ru (R.A. Simonyan), margarita_kardashyan@mail.ru (M.A. Kardashyan)

2. Обсуждение

Размытый образ злоумышленника, который может быть получен в результате применения процедур первоначального поиска, будем называть размытым образом злоумышленника нулевого поколения или базового поколения. При достаточно большом количестве данных, включенных как в специализированную базу знаний о злоумышленных действиях (шаблонах), так и в специализированную базу знаний о штатных ситуациях и значений их допустимых характеристик, эвристические алгоритмы первоначального поиска в основном могут обеспечить некоторое значимое положительное значение функциональной эффективности поиска. Вместе с тем ряд причин не позволяет при первоначальном поиске достичь того уровня функциональной эффективности, при котором непосредственный анализ размытого образа злоумышленника первого поколения позволяет получить достоверную и оперативную информацию о злоумышленном или потенциально возможном злоумышленном действии. Такими причинами обычно являются: 1) недостаточная информативность данных как в специализированной базе знаний о злоумышленных действиях (шаблонах), так и специализированной базе знаний о штатных ситуациях и значений их допустимых характеристик; 2) эвристический характер алгоритмов первоначального поиска размытого образа злоумышленника; 3) наличие большого количества неопределенностей у признаков, описывающих образы злоумышленников; 4) невозможность учета алгоритмами первоначального поиска различных зависимостей между признаками и т.д. Таким образом возникает необходимость построения размытых образов злоумышленника, обеспечивающих более высокую функциональную эффективность их определения. Это можно сделать с помощью метода итераций, т.е. метода последовательных приближений (Панюкова, 2013; Ченцов, 2016). Будем считать, что на t-ом шаге итерации на основе анализа размытого образа злоумышленника (t-1)-го поколения строится размытый образ злоумышленника t-го поколения.

Процедура построения размытого образа злоумышленника t-го поколения условно может быть разбита на три этапа.

На первом этапе генерируются различные обобщенные факторы, влияющие на возникновение потенциально возможное проявление каналов утечки информации. Для каждого из этих факторов вычисляются значения функции сходства между размытым образом злоумышленника (t-1)-го поколения и размытым подмножеством, функция принадлежности которому i-го образа из базы знаний принимает значение, равное значению рассматриваемого фактора у i-го образа злоумышленника. Факторы, соответствующие значения функции сходства которых выше некоторого порогового значения, включаются в список обобщённых факторов наиболее характерных для нечеткого образа злоумышленника (t-1)-го поколения.

На втором этапе специалисту по защите информации для корректировки выдаётся полученный список наиболее характерных факторов. Специалистом из списка исключаются факторы, неприемлемые вследствие плохой интерпретируемости. Специалистом могут быть также добавлены в список некоторые новые факторы, которые хотя и не были включены в список на t этапе, однако специалистом считаются характерными для нечеткого образазлоумышленника (t-1)-го поколения.

На третьем этапе на основе скорректированного списка наиболее характерных факторов и размытого образа злоумышленника предыдущего (t-1)-го поколения, с помощью композиции строится образ злоумышленника t-го поколения.

Рассмотрим детальнее первый этап. Хотя предлагаемая методика построения размытого образа злоумышленника t-го поколения этого не требует, далее, говоря об обобщённых факторах, будем ограничиваться рассмотрением так называемых дихотомических обобщённых факторов, которые можно выразить в виде некоторой логической функции от описывающих образы злоумышленников дихотомических признаков.

Предлагаемые далее алгоритм генерации обобщённых факторов не использует никаких содержательных сведений о признаках, составляющих факторы, способствующих возникновению каналов утечки информации, кроме знаний о том, какие дихотомические признаки представляют один качественный признак, характеризующий наличие злоумышленника. Конечно, это снижает «интеллектуальные» возможности блока

генерации, поскольку в противном случае «понимая» смысл дихотомических признаков, зная зависимости между ними, блок мог бы иногда сократить перебор, например, повторно не рассматривая подобные обобщённые факторы и т. д. Однако, с другой стороны, возможно, что исключение содержательных сведений о признаках в некоторых случаях будет приводить к выявлению неочевидных для нормальной логики службы защиты информации аналогий и обобщений, обнаружение которых присуще мышлению некоторого типа нестандартных злоумышленников. Это обстоятельство при анализе данных может оказаться полезным, поскольку способность нахождения злоумышленников при проявлении неочевидных аналогий, является отличительной чертой службы защиты информации, т.е. благодаря способности сотрудников к неожиданным сопоставлениям.

Другим преимуществом, предлагаемого блока генерации факторов, является независимость алгоритма работы от конкретного исходного множества данных в базах знаний. Отсутствие содержательных сведений позволяет использовать без изменений рассматриваемую итеративную процедуру не только в области информационной безопасности, но и в области управления большими системами, социологии, медицины и в ряде других областей, где архивные данные могут быть представлены в дихотомизированном виде (Шуметов, 2013; Бабичев, 2013).

В зависимости от множества элементарных логических операций, допустимых при конструировании генерируемого фактора, будет изменятся и класс рассматриваемых факторов. Однако, не всякая логическая функция от дихотомических переменных f_i^j может считаться обобщённым фактором. Для этого она должна удовлетворять одному существенному требованию: она должна быть простой. Это требование, во-первых, обосновывается большим количеством фактов из истории имевших место нарушений защиты информации в АСОД, откуда видно, что реальные нарушения, порой новые и совершенно неочевидные, описываются в основном простыми факторами (Николаенко, 2015; Выпасняк, 2013; Лопатин, 2013). Во-вторых, оперирование простыми обобщенными факторами позволяет за счет доступности их интерпретации создавать, например, диалоговые процедуры оперативно-диспетчерского управления защитой информации (Симаворян, 2015), диалоговые процедуры обучения службы защиты информации (Симаворян, 2014). В-третьих, сложные факторы за счет слишком детального описания размытого образа злоумышленникане дают хорошей «экстраполяции», т.е. «обобщенности».

Поскольку попытки определить понятие “простоты” факторов, влияющих на возникновение каналов утечки информации, требуют дополнительного обоснования, в качестве приемлемых с практической точки зрения, тривиальных характеристик простоты можем использовать, например, число дихотомических признаков, входящих в обобщенный фактор, или множество элементарных логических операций, допустимых при конструировании фактора и многое другое (Шуметов, 2013). Если число дихотомических признаков, входящих в обобщенный фактор, принять равным l, а в качестве допустимых логических операций взять дизъюнкцию, конъюнкцию и отрицание, то число различных обобщенных факторов будет равно $C_m{}^l \cdot 2^{2^l}$. Так, если образы объектов описываются, например, 50 дихотомическими признаками, а l принять равным 3, то количество обобщенных факторов будет более $5*10^6$. К тому же далеко не все из них можно считать “простыми”.

Для того, чтобы генерируемые обобщенные факторы были бы более “простыми” и чтобы уменьшить их число, можно предварительно для каждого качественного признака f_i ввести дополнительные признаки φ_i^1, φ_i^2,..., которые представляют собой всевозможные дизъюнкции нескольких f_i^j и f_i^l, причем число составляющих каждого из признаков φ_i^1, φ_i^2,... дихотомических признаков и их отрицаний ограничить сверху некоторым числом α. После введения дополнительных признаков, в качестве обобщенных факторов следует исследовать либо f_i^j, либо f_q^l, либо φ_g^p , либо не более чем β - местные конъюнкции от f_i^j, f_q^l и φ_g^p.

Хотя введенные ограничения позволяют уменьшить трудоемкость работы блока, генерирующего обобщенные факторы, в зависимости от значений m, m_i, α и β в некоторых случаях бывает целесообразным с помощью различных эвристических приемов сократить перебор. С этой целью, во–первых, для каждого качественного признака f_i будем вводить не

$\sum_{j=2}^{\alpha} Cm_j^j \cdot 2^j$ дополнительных признаков $\varphi^p{}_j$, а гораздо меньше, за счет введения лишь признаков, составляющие элементы которых являются достаточно характерными для образа злоумышленника (t-1)-го поколения. Во-вторых, при генерации обобщенных факторов будут генерироваться не всевозможные конъюнкции от f_i^j, $\bar{f}_q^l$, $\varphi_g{}^p$, а лишь такие, составляющие элементы которых уже являются достаточно характерными для образа злоумышленника (t-1)-го поколения.

Для упрощения описания алгоритма генерации обобщенных факторов, основанного на приведенных эвристических приемах, предположим, что существует некоторая память, состоящая из S пар ячеек, причем в первые ячейки пар записываются различные логические выражения от $f_i{}^j$ и $\bar{f}_q^l$, а во вторые ячейки записываются значения функции сходства между подмножеством образов из базы данных, на которых записанные в первых ячейках логические выражения принимают значение “истинно”, и размытым подмножеством, соответствующим нечеткому образу злоумышленника (t-1)-го поколения. При описании алгоритма будем также предполагать, что существует некоторая процедура, далее называемая «пороговым запоминанием», суть которой в следующем: если не все S ячеек памяти заняты, то при пороговом запоминании некоторого логического выражения, в первую ячейку первой свободной пары ячеек записывается это выражение, а во вторую – соответствующее значение функции сходства с нечетким образом злоумышленника. В том случае, когда в пороговой памяти свободных ячеек нет, то предварительно вычисляется соответствующее рассматриваемому логическому выражению значение сходства, и если это значение оказывается меньше всех значений, записанных, во вторых ячейках пар памяти, то содержимое памяти не изменяется. Если же в памяти существует хотя бы одно значение, которое меньше рассматриваемого, то на место логического выражения из памяти, которому соответствует наименьшее значение функции сходства, записывается рассматриваемое логическое выражение. При этом соответственным образом изменяется и содержимое второй ячейки пары.

Перейдем к описанию алгоритма генерации дополнительных признаков φ_i^p для качественного признака f_i:

пусть p – переменная, которая показывает одно- или двухместные дизъюнкции, которые будут генерироваться на данном этапе, q – переменная, которая показывает какая пара ячеек памяти будет обрабатываться, S – память.

Алгоритм I.

Шаг I. Осуществить пороговое запоминание дизъюнкций

$f_i^j \vee f_i^l$ и $\bar{f}_i^j \vee \bar{f}_i^l$ где $j = 1,2, \dots m_{i-1}; l = j+1, j+2, \dots m_i$

и дизъюнкций

$f_i^j \vee \bar{f}_i^l$ где $l = 1,2, \dots m_i;\ j = 1,2, \dots m_i; j \neq l$

Шаг 2. p =3

Шаг 3. q=1

Шаг 4. Если $q > S$, т. е. просмотр всей памяти закончен, то перейти к шагу 7.

Шаг 5. Если логическое выражение, записанное в первой ячейке q-той пары является (p-1) - местной дизъюнкцией, то φ^* приравнять к этой дизъюнкции и перейти к следующему шагу. В противном случае: $q = q + 1$, и перейти к шагу 4.

Шаг 6. Для $l = 1,2, \dots m_i$, если ни f_i^l, ни $\bar{f}_i^l$ не входят в φ^*, осуществить пороговое запоминание дизъюнкций $\varphi^* \vee f_i^l$ и $\varphi^* \vee \bar{f}_i^l$, q=q+1.Перейти к шагу 4.

Шаг 7. $p = p + 1$. Если $p \leq \alpha$, то перейти к шагу 3.

Шаг 8. На этом шаге должен быть осуществлен выбор: какие из дизъюнкций будут введены в качестве дополнительных признаков. Тут возможны два подхода. Согласно первому, в качестве дополнительных признаков следует брать те дизъюнкции, соответствующие значения функции сходства с нечетким образом злоумышленника (t-1)-го поколения больше некоторого порогового значения. При втором подходе в качестве дополнительных признаков вводятся заранее определенное количество дизъюнкций с максимальными значениями функции сходства с размытым образом злоумышленника (t-1)-го поколения. При практической реализации этого алгоритма необходимо пользоваться

подходом, в котором заранее определяется, что для каждого качественного признака f_i, должно вводиться m_i дополнительных признаков.

Шаг 9. Конец.

Естественно, что чем больше число парных ячеек памяти S, тем больше и время работы, и точность работы. При проведении многочисленных экспериментов рекомендуется брать $S=\alpha * m_i$.

Приведем также алгоритм генерации обобщённых факторов. Ниже g_l обозначает число дополнительных признаков φ_l^1, φ_l^2, ..., сгенерированных алгоритмом 1 для качественного признака f_l.

Алгоритм 2.

Шаг 1. Осуществить пороговое запоминание конъюнкций

$f_i^j \wedge f_l^p$ и $\overline{f}_i^j \wedge f_l^p$, где $i = 1, 2, ..., k$, $j = 1, 2, ..., m_i$, $l = i+1, i+2, ..., k$, $p = 1, 2, ..., m_l$.

$f_i^j \wedge \overline{f}_l^p$, где $i = 1, 2, ..., k$; $j = 1, 2, ..., m_i$; $l = 1, 2, ..., k$; $l \neq i$; $p = 1, 2, ..., m_l$.

$\overline{f}_i^j \wedge \varphi_l^p$ и $f_i^j \wedge \varphi_l^p$, где $i = 1, 2, ..., k$; $j = 1, 2, ..., m_i$; $l = 1, 2, ..., k$; $l \neq i$; $p = 1, 2, ..., g_l$.

$\varphi_i^p \wedge \varphi_l^j$, где $i = 1, 2, ..., k$; $p = 1, 2, ..., g_i$; $l = 1, 2, ..., k$; $l \neq i$; $j = 1, 2, ..., g_j$.

Шаг 2. $p = 3$

Шаг 3. $q = 1$

Шаг 4. Если $q > S$, перейти к шагу 8.

Шаг 5. Если логическое выражение, записанное в первой ячейке q-той пары является (p-1)-местной конъюнкцией, то φ^* приравнять к этой конъюнкции и перейти к следующему шагу. В противном случае: $q = q + 1$ и перейти к шагу 4.

Шаг 6. Для $i = 1, 2, \ldots k$ и $l = 1, 2, \ldots m_i$, если ни f_i^l, ни $\overline{f}_i^l$ не входит в φ^*, осуществить пороговое запоминание конъюнкций $\varphi^* \wedge f_i^l$ и $\varphi^* \wedge \overline{f}_i^l$.

Шаг 7. Для $i = 1, 2, \ldots k$ и $l = 1,2,\ldots g_i$, если φ_i^l не входит в φ^*, осуществить пороговое запоминание конъюнкции $\varphi^* \wedge f_i^l$.

Шаг 8. $p = p + 1$. Если $p \leq \beta$, то перейти к шагу 3.

Шаг 9. Осуществить пороговое запоминание φ_i^p, f_i^j и $\overline{f}_i^j$, где $i = 1, 2, ..., k$; $j = 1, 2, ..., m_i$; $p = 1, 2, ..., g_i$.

Шаг 10. Логические выражение, соответствующие значениям функции сходства для которых выше некоторого заранее заданного порога выдать службе защиты информации, как наиболее характерные для образа злоумышленника (t-1)-го поколения.

Шаг 11. Конец.

В практической реализации этого алгоритма целесообразнобрать $S=\beta * m_i$.

3. Результаты

Предложенные два алгоритма поиска злоумышленников с помощью метода итераций представляют большой практический интерес. Их практическая реализация позволит последовательно и планомерно на регулярной основе обнаруживать потенциально возможные злоумышленные (как преднамеренные, так и не преднамеренные) действия.

4. Заключение

Для реализации предложенных алгоритмов требуется большое количество исходных данных. Эти данные могут быть созданы на базах знаний: 1) специализированной базы знаний о злоумышленных действиях, элементы которой называются шаблонами; и 2) специализированной базы знаний о штатных ситуациях и допустимых их характеристиках. В силу закрытости многих методов и данных, по имеющимся и прогнозируемым злоумышленным действиям, предложенные алгоритмы имеют практический интерес для многих служб защиты информации на различных автоматизированных системах обработки данных.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-01-00527.

Литература

Бабичев, 2013 - Бабичев А.В. (2013). О Согласовании поведения взаимодействующих объектов / Управление большими системами: сборник трудов. № 46. С. 6-67.

Выпасняк и др., 2013 - Выпасняк В.И., Тиханычев О.В., Гахов В.Р. (2013). Кибер-угрозы автоматизированным системам управления. // Вестник академии военных наук. № 1 (42). С. 103-109.

Лопатин и др., 2013 - Лопатин Д.В., Анурьева М.С., Еремина Е.А., Заплатина Е.А., Калинина Ю.В. (2013). Информационно-коммуникационные угрозы. //Психолого-педагогический журнал Гаудеамус. № 2 (22). С. 148-155.

Николаенко и др., 2015 - Николаенко М.А., Иваницкий А.В., Гребенник О.Г. (2015). Статистический анализ хакерских атак русского сегмента интернета за первую половину 2015 года. // Теория и практика современной науки. № 6 (6). С. 935-937.

Панюкова, 2013 - Панюкова Т.А. (2013). Численные методы. Изд.стереотип. URSS. 224 с.

Симаворян и др., 2013 - Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян Р.А. (2013). Системный подход к проектированию интеллектуальных систем защиты информации // «Известия Сочинского государственного университета», № 4-2(28), С. 128-132.

Симаворян и др., 2014 - Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. (2014). Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД. // Известия СГУ, № 4-1 (32). С. 15-23.

Симаворян и др., 2015 - Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. (2015). Разработка алгоритма принятия решений по оперативно-диспетчерскому управлению средствами защиты информации на основе методов искусственного интеллекта. // «Modeling of Artificial Intelligence», Vol (5), Is. 1, p. 33- 41.

Ченцов, 2016 - Ченцов А.Г. (2016). Метод программных итераций в игровой задаче наведения. // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. Т. 26. № 2. С. 271-282.

Шуметов, Крюкова, 2013 - Шуметов В.Г., Крюкова О.А. (2013). Методология и практика анализа данных в управлении. Методы одномерного и двумерного анализа. // Монография. Издательство: Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Орел, ISBN: 978-5-93179-326-9. С. 177.

Simavoryan et al., 2014 - Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. (2014). About one approach to a question of classification of intellectual system of information security // «Modeling of Artificial Intelligence», Vol (1), Is 1, p. 29-44.

References

Babichev, 2013 - Babichev A.V. (2013). O Soglasovanii povedeniya vzaimodeistvuyushchikh ob"ektov / Upravlenie bol'shimi sistemami: sbornik trudov. № 46. S. 6-67.

Vypasnyak i dr., 2013 - Vypasnyak V.I., Tikhanychev O.V., Gakhov V.R. (2013). Kiber-ugrozy avtomatizirovannym sistemam upravleniya. // Vestnik akademii voennykh nauk. № 1 (42). S. 103-109.

Lopatin i dr., 2013 - Lopatin D.V., Anur'eva M.S., Eremina E.A., Zaplatina E.A., Kalinina Yu.V. (2013). Informatsionno-kommunikatsionnye ugrozy. //Psikhologo-pedagogicheskii zhurnal Gaudeamus. № 2 (22). S. 148-155.

Nikolaenko i dr., 2015 - Nikolaenko M.A., Ivanitskii A.V., Grebennik O.G. (2015). Statisticheskii analiz khakerskikh atak russkogo segmenta interneta za pervuyu polovinu 2015 goda. // Teoriya i praktika sovremennoi nauki. № 6 (6). S. 935-937.

Panyukova, 2013 - Panyukova T.A. (2013). Chislennye metody. Izd.stereotip. URSS. 224 s.

Simavoryan i dr., 2013 - Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. (2013). Sistemnyi podkhod k proektirovaniyu intellektual'nykh sistem zashchity informatsii. // «Izvestiya Sochinskogo gosudarstvennogo universiteta», № 4-2(28), S. 128-132.

Simavoryan i dr., 2014 - Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. (2014). Issledovanie intellektual'nogo protivoborstva zloumyshlennikov i sluzhby zashchity informatsii v ASOD. // Izvestiya SGU, № 4-1 (32). C. 15-23.

Simavoryan i dr., 2015 - Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. (2015). Razrabotka algoritma prinyatiya reshenii po operativno-dispetcherskomu upravleniyu sredstvami zashchity informatsii na osnove metodov iskusstvennogo intellekta. // «Modeling of Artificial Intelligence», Vol (5), Is. 1, p. 33- 41.

Chentsov, 2016 - Chentsov A.G. (2016). Metod programmnykh iteratsii v igrovoi zadache navedeniya. // Vestnik Udmurtskogo universiteta. Matematika. Mekhanika. Komp'yuternye nauki. T. 26. № 2. S. 271-282.

Shumetov, Kryukova, 2013 - Shumetov V.G., Kryukova O.A. (2013). Metodologiya i praktika analiza dannykh v upravlenii. Metody odnomernogo i dvumernogo analiza. // Monografiya. Izdatel'stvo: Rossiiskaya akademiya narodnogo khozyaistva i gosudarstvennoi sluzhby pri Prezidente Rossiiskoi Federatsii, Orel, ISBN: 978-5-93179-326-9. S. 177.

Simavoryan et al., 2014 - Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. (2014). About one approach to a question of classification of intellectual system of information security // «Modeling of Artificial Intelligence», Vol (1), Is 1, p. 29-44.

УДК 681.3

Повышение функциональной эффективности поиска нечеткого образа злоумышленника методом итераций

Симон Жоржевич Симаворян [a, *], Арсен Рафикович Симонян [a], Елена Ивановна Улитина [a], Виктор Иванович Самарин [a] , Рафик Арсенович Симонян [b], Маргарита Аркадьевна Кардашян [a]

[a] Сочинский государственный университет, Российская Федерация,
[b] Кубанский государственный университет, Российская Федерация

Аннотация. Работа посвящена разработке методов поиска нечеткого образа злоумышленника на основе использования метода итераций. Поиск осуществляется на данных из специализированной базы знаний о злоумышленных действиях (шаблонах) и базы знаний о штатных ситуациях и значений их допустимых характеристик.

Ключевые слова: нечеткий образ злоумышленника, метод итераций.

* Корреспондирующий автор
Адреса электронной почты: simsim58@mail.ru (С.Ж. Симаворян), oppm@mail.ru (А.Р. Симонян), elenaulitina@mail.ru (Е.И. Улитина), visamarin@mail.ru (В.И. Самарин), raf55@list.ru (Р.А. Симонян), margarita_kardashyan@mail.ru (М.А. Кардашян)