Алгоритмы поддержки принятия решений как способ совмещения различных политик безопасности

Н.Ф. Богаченко
nfbogachenko@mail.ru

Ю.С. Ракицкий
yrakitsky@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

Задача совмещения нескольких политик безопасности в единой информационной системе является актуальной проблемой с точки зрения администрирования компьютерных систем. В современных стандартах обеспечения информационной безопасности компьютерных систем присутствует требование наличия не менее чем двух политик безопасности. Существующие методы решения данной задачи сводятся к поиску решения, при котором настройки всех совместно используемых политик безопасности являются непротиворечивыми. В реальных системах не всегда возможно найти соответствующие настройки. Также не доказан факт существования идеального решения. Одним из перспективных путей решения сформулированной задачи является подход, основанный на алгоритмах поддержки принятия решений.

Введение

В современных компьютерных системах часто возникает необходимость строго разграничить права доступа. При этом разграничение доступа может осуществляться в соответствии с несколькими политиками безопасности. Многие стандарты защиты информации предполагают использование нескольких политик разграничения доступа. Например, в "Оранжевой книге"наличие только одной дискреционной политики разделения доступа позволит отнести компьютерную систему к какому-либо из классов безопасности группы "C тогда как совместное использование дискреционного и мандатного контроля доступа в компьютерной системе позволяет достигать более высоких классов защищенности групп "B"или "A". При этом "Оранжевой книгой"подразумевается именно совмещение мандатной и дискреционной политики безопасности, наличие только мандатной политики безопасности в компьютерной системе не позволит отнести ее к какому-либо классу "Оранжевой книги". В качестве еще одного примера совмещения нескольких политик безопасности можно привести некоторые системы управления базами данных. Если такие системы управления базами данных функционируют на базе операционной системы из семейства Windows, то применяемая в системах управления базами данных ролевая политика безопасности определяет доступ пользователей к записям базы данных, но при этом сами записи хранятся в файлах. Доступ же к файлам регулируется операционной системой. В операционных системах семейства Windows основой разграничения доступа является дискреционная политика безопасности. Также в современных версиях операционных систем семейства Windows реализованы уровни целостности, которые представляют собой мандатную политику

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data Analysis and Modelling (DAM 2016), Omsk, Russia, October 2016, published at http://ceur-ws.org

безопасности. Таким образом, необходимо совместить требования трех различных политик безопасности в одной системе.

Стандартный подход к решению описанной проблемы – поиск идеального решения, при котором запреты и разрешения одной политики безопасности не противоречат другой политике безопасности. С использованием данного подхода были представлены различные решения. Работы [1, 2] описывают совместную реализацию ролевой и мандатной моделей разграничения доступа. Использование теоретико-графового подхода к описанию решеток ценностей мандатной политики безопасности позволило совместить требования ролевой и мандатной моделей разграничения доступа, благодаря построению орграфа сущностей компьютерной системы. Представлен алгоритм совмещения ролевой и мандатной политик безопасности. Авторы работы [3] предлагают преобразовать матрицу доступов, изменив ее базовые координаты: правила доступа установлены не между субъектом и объектом, а между "субъектом доступа, запрашивающим доступ к объекту"и "субъектом доступа, создавшим этот объект". Показано, что такой подход позволяет реализовать и использовать дискреционную и мандатную политики безопасности совместно. В работе [4] рассмотрено расширение дискреционной модели Take-Grant, принимающее во внимание механизм мандатного разграничения доступа. В статье [5] предложен универсальный язык, позволяющий описать и реализовать глобальную интегрированную политику безопасности для системы, состоящей из множества информационных сред, каждая из которых имеет уникальную модель обеспечения безопасности и домен администрирования. Реализация этого языка позволяет получить монитор событий. Разрешение конфликтов, возникающих вследствие противоречий в настройках различных политик безопасности осуществляется путем явного вызова администратора для принятия приоритетного решения. В работе [6] матрицу доступов дискреционной политики безопасности предлагается расширить до куба доступов, в котором помимо традиционных субъектов и объектов добавлена третья размерность - пользователи или группы пользователей. Эта дополнительная размерность позволяет организовать механизм группового управления доступом, тем самым реализуя ролевую политику безопаснсти и оставаясь в рамках дискреционной политики безопасности. В работе [7] представлена модель управления доступом для работы с XML-документами. В этой модели объединены преимущества ролевой и мандатной политик разграничения доступа. В частности, для определения прав доступа предлагается использовать не списки управления доступом, а подход, основанный на метках безопасности.

Тем не менее, существует фундаментальная проблема реализации идеального подхода, заключающаяся в отсутствии доказательств того, что существует идеальное решение. Кроме того, практическая реализация одновременного введения множественной политики безопасности показывает, что не всегда можно внести изменения, чтобы обеспечить надлежащее функционирование системы. В данной статье рассматривается новый подход к совмещению нескольких политик безопасности в одной компьютерной системе, основанный на алгоритме поддержки принятия решений.

1 Постановка задачи и общий подход к решению

Рассмотрим систему, в которой, в качестве механизмов разграничения доступа, присутствуют дискреционная и мандатная политики безопасности. Исторически сложилось общепринятое мнение, которое лежит в основе практически всех стандартов защиты информации, мандатная политика безопасности является более высокоуровневым механизмом защиты информации, а дискреционная политика безопасности необходима для реализации базового уровеня защиты данных. В результате, правила, заданные мандатной политикой безопасности, доминируют над правилами дискреционной политики безопасности. При возникновении конфликтов между правилами, заданными двумя политиками безопасности обычно используется один из двух подходов. Первый подход предполагает, что если присутствует запрет на действие в правилах хотя бы одной политики, то доступ запрещен. Второй подход основан на доминирующем положении мандатной политики безопасности , и решение о предоставлении доступа принимается исходя из заданных ею правил. Первый подход может приводить к необоснованным отказам в доступе и, как следствие, к полной неработоспособности системы. Второй подход предполагает, что все решения о разрешениях и запретах доступа будет принимать мандатная политика безопасности, дискреционная политика при этом практически не используется. Более того, мандатная политика безопасности реализует принудительное управление доступом, следовательно, ориентирована на систему в целом. Администратор задает метки безопасности субъектов и объектов системы, которые не могут изменяться при попытках доступа, изменения возможны только при принятии администратором решения перераспределить метки безопасности. Но, при этом, возможны исключительные ситуации. Например, администратору нужно предоставить доступ определенного

субъекта к определенному объекту, но мандатная политика безопасности противоречит такому доступу. Администратор имеет возможность следить за содержимым объекта и может гарантировать отсутствие утечки информации через субъект, которому предоставлен доступ, но не может гарантировать отсутствия утечки информации через субъекты, которым предоставлен аналогичный уровень доступа. Выдачу данного разрешения возможно реализовать с помощью введения некоторых дополнительных меток безопасности для каждого подобного случая, но очевидно, что такой подход приведет к существенному увеличению и запутыванию решетки ценностей и, следовательно, к усложнению выполнения административных функций. Другой подход состоит в использовании дискреционной политики безопасности, которая в определенных случаях должна доминировать над мандатной политикой безопасности. Другими словами, в системе нужно создать механизм, который принимает решение о доминировании той или иной политики безопасности в каждом конкретном случае.

Формализуем постановку задачи. Пусть алгоритмы S_1 и S_2 принимают решение для двух политик безопасности, заданных в системе. Необходимо реализовать дополнительный алгоритм S, который при каждой попытке доступа должен принять решение о том, правила какой политики безопасности применить в данном случае. При этом алгоритм S срабатывает только в том случае, когда результаты работы алгоритмов S_1 и S_2 противоречат друг другу.

В рамках одной отдельно взятой политики безопасности для определения возможности доступа необходимо принять решение из множества $\{0, 1\}$, где нулевое значение означает отказ в доступе, а единичное - разрешение. В случае, когда в системе присутствует две или более политик безопасности, значений указанного множества будет недостаточно. Необходимо расширить область значений алгоритма принятия решений до множества $\{-T, ..., -1, 0, 1, ..., T\}$, где T - целое положительное число. Значения из данного интервала будем называть уровнем разрешения и обозначать буквой t. Доступ разрешен, если $t \geq 0$. Чем выше уровень разрешения t, тем выше степень доверия к доступу. Уровень разрешения можно сопоставить с вероятностью утечки информации при конкретном доступе: чем выше вероятность p, тем меньший уровень разрешения t необходимо назначить. Также можно утверждать, что количественная оценка уровня разрешения t - это априорная информация о возможности утечки информации при запрашиваемом доступе. При первом приближении получим формулу: $p = 0,5 - (t/2T)$.

При предложенном подходе решение о предоставлении доступа тем или иным алгоритмом (например, дискреционной или мандатной политикой безопасности) принимается на основе результата вычисления соответствующего уровня разрешения. При этом алгоритму S необходимо принимать решение t, исходя из уровней разрешения t_1 и t_2 отдельных политик безопасности S_1 и S_2. Введем коэффициент доминирования r, показывающий во сколько раз решение, принимаемое политикой безопасности S_1, более значимо, чем решение, принимаемое политикой S_2. В этом случае окончательное решение может быть вычислено как взвешенная сумма решений двух политик безопасности:

$$t = \frac{r}{r+1} t_1 + \frac{1}{r+1} t_2. \tag{1}$$

Равнозначность политик безопасности достигается при $t = 1$. При этом, t не обязательно является целым числом, важное значение имеет только присутствие значения t в интервале: $t \in [-T, T]$.

2 Совмещение мандатной и дискреционной политик безопасности

Рассмотрим часто встречающуюся ситуацию совмещения мандатной и дискреционной политик безопасности.

Для мандатной политики безопасности ограничимся наиболее часто встречающимся и простым случаем линейной решетки ценностей, содержащей L уровней безопасности. В таких условиях уровень разрешения может быть найден как разность между уровнем доверия субъекта $C(S)$ и уровнем секретности объекта $C(O)$:

$$t_1 = (C(S) - C(O)) \frac{T}{L-1}. \tag{2}$$

Так как $C : S \cup O \to \{0, ..., L-1\}$ (S - множество субъектов, O - множество объектов), то $t_1 \in [-T, T]$.

Для дискреционной политики безопасности уровень разрешения может устанавливаться произвольно администратором для каждого доступа. Если администратор хочет предоставить доступу наивысший приоритет, то он присваивает значение $t_2 = T$. Поэтому ограничимся случаем назначения уровня разрешения

по умолчанию. В системе должно быть задано общее количество возможных видов доступа, пусть в нашем случае оно равно M. Пусть субъект запрашивает доступ к объекту сразу на несколько видов доступа. Если в доступе отказано, то будем считать, что

$$t_2 = -k\frac{T}{M}, \tag{3}$$

где k - количество запрещенных доступов из списка запрашиваемых доступов. Если доступ разрешен, то положим

$$t_2 = h\frac{T}{M}, \tag{4}$$

где h - количество разрешенных, но не запрашиваемых видов доступа.

При совмещении мандатной и дискреционной политик безопасности был рассмотрен простейший случай линейной решетки ценностей. Однако в реальных системах мандатная политика безопасности может быть задана нелинейной решеткой ценностей, т.е. множество меток безопасности будет являться частично упорядоченным. При таком подходе к реализации политик безопасности может возникнуть ситуация, при которой уровень доверия субъекта $C(S)$ и уровень секретности объекта $C(O)$ окажутся несравнимыми. В этом случае определить уровень разрешения как разность между уровнем доверия субъекта $C(S)$ и уровнем секретности объекта $C(O)$ (см. формулу 2) нельзя. Это означает, что нужен другой подход к определению уровня разрешения, задаваемого мандатной политикой безопасности.

Классическая модель мандатной политики безопасности определяет оператор $sup(,)$, задающий для любой пары элементов l_1 и l_2 из базового множества уровней безопасности SX единственный элемент наименьшей верхней границы: $sup(l_1, l_2) = l$ тогда и только тогда, когда $(l_1 \leq l) \wedge (l_2 \leq l) \wedge (\forall l' \in SX : ((l_1 \leq l') \wedge (l_2 \leq l')) \Rightarrow (l \leq l'))$. Введем оператор $dif(,)$, показывающий крастояниень от уровня безопасности l_1 до наименьшей верхней границы уровней безопасности $l_1, l_2 : dif(l_1, sup(l_1, l_2)) = sup(l_1, l_2) - l_1$. Такой подход возможен, поскольку элементы решетки l_1 и $sup(l_1, l_2)$ будут всегда сравнимы по определению. Данный оператор позволяет определить количество уровней решетки ценностей от элемента l_1 до $sup(l_1, l_2)$. Отметим, что данная величина всегда будет неотрицательной.

Будем определять уровень разрешения t_1 для несравнимых в решетке уровня доверия субъекта $C(S)$ и уровня секретности объекта $C(O)$ как отрицательный модуль разностей расстояний уровня доверия субъекта $C(S)$ и уровня секретности объекта $C(O)$ до наименьшей верхней границы $sup(C(S), C(O))$:

$$t_1 = -1|(dif(C(S), sup(C(S), C(O))) - dif(C(S), sup(C(S), C(O))))|\frac{T}{H}, \tag{5}$$

здесь H - максимальное значение оператора dif. Очевидно, что $0 \leq H \leq (L-1), L = |SX|$.

В случае, когда уровень доверия субъекта $C(S)$ и уровень секретности объекта $C(O)$ являются несравнимыми, доступ не предоставляется, поэтому величина должна быть отрицательной. При этом, поскольку определяется разность "расстояний"между уровнями в решетке, вычисляется абсолютное значение разности.

3 Применение метода анализа иерархий

Часто в одной системе действуют не по одной, а сразу по две мандатных и дискреционных политик безопасности: одна пара связана с конфиденциальностью, а другая - с целостностью. В этом случае для вычисления уровня разрешения удобнее воспользоваться методом анализа иерархий со следующим деревом решения: вершина иерархии - уровень разрешения t; критерии: ДПБ и МПБ - дискреционная и мандатная политики безопасности; альтернативы: политика целостности и политика конфиденциальности. Отметим, что метод анализа иерархий достаточно часто применяется для решения задач в области информационной безопасности, например, в статьях [8, 9, 10] метод был использован для построения модели ролевого разграничения доступа.

При использовании метода анализа иерархий необходимо заполнить три матрицы парных сравнений: одна - для уровня критериев и две - для уровня альтернатив. Пусть, в соответствии с вышеизложенным, $r(r > 0)$ - коэффициент доминирования, показывающий во сколько раз решение, принимаемое мандатной политикой безопасности (МПБ), более значимо, чем решение дискреционной политики (ДПБ). Предпочтительность политики конфиденциальности по сравнению с политикой целостности можно оценить двумя

аналогичными параметрами: $r_1(r_1 > 0)$ - для дискреционной модели, $r_2(r_2 > 0)$ - для мандатной модели. Тогда матрицы парных сравнений задаются таблицей 1.

Таблица 1: Матрицы парных сравнений

t	ДПБ	МПБ
ДПБ	1	$1/r$
МПБ	r	1

ДПБ	цел.	конф.
цел.	1	$1/r_1$
конф.	r_1	1

МПБ	цел.	конф.
цел.	1	$1/r_2$
конф.	r_2	1

Согласованность этих матриц является следствием того, что для двумерной обратно симметричной матрицы M всегда выполняется условие: $\forall i, j, k$ имеет место равенство $[M]_{ij} = [M]_{ik} \times [M]_{kj}$. В таком случае относительные весовые коэффициенты определяются нормированными столбцами всех трех матриц парных сравнений, а формулы для вычисления относительных приоритетов политики целостности и политики конфиденциальности принимают следующий вид:

$$R^{\text{цел}} = \frac{1}{1+r_1} \times \frac{1}{1+r} + \frac{1}{1+r_2} \times \frac{r}{1+r}, R^{\text{конф}} = \frac{r_1}{1+r_1} \times \frac{1}{1+r} + \frac{r_2}{1+r_2} \times \frac{r}{1+r} = 1 - R^{\text{цел}}. \quad (6)$$

Окончательное решение о предоставлении доступа теперь может быть вычислено по формулам:

$$t = R^{\text{цел}} \times t^{\text{цел}} + R^{\text{конф}} \times t^{\text{конф}}, t^{\text{цел}} = \frac{1}{1+r} t^{\text{цел}}_{\text{ДПБ}} + \frac{r}{1+r} t^{\text{цел}}_{\text{МПБ}}, t^{\text{конф}} = \frac{1}{1+r} t^{\text{конф}}_{\text{ДПБ}} + \frac{r}{1+r} t^{\text{конф}}_{\text{МПБ}}, \quad (7)$$

где верхний индекс означает политику конфиденциальности или целостности, а нижний - дискреционное или мандатное разграничение доступа. Пары величин $t^{\text{цел}}_{\text{ДПБ}}$ $t^{\text{цел}}_{\text{МПБ}}$ и , а также $t^{\text{конф}}_{\text{ДПБ}}$ и $t^{\text{конф}}_{\text{МПБ}}$ вычисляются аналогично паре уровней разрешения t_1 и t_2 по алгоритму S, изложенному в разделе 2. Анализируя полученные формулы, можно сделать следующие выводы:

1. Так как $R^{\text{цел}}$ и $R^{\text{конф}}$ принадлежат интервалу $(0, 1)$, то применение метода анализа иерархий в тех случаях, когда величины $t_{\text{цел}}$ и $t_{\text{конф}}$ имеют одинаковые знаки не изменит решение о предоставлении доступа.

2. Если $r_1 \geq 1$ и $r_2 \geq 1$, то $R^{\text{цел}} \leq R^{\text{конф}}$. Если $r_1 < 1$ и $r_2 < 1$, то $R^{\text{цел}} > R^{\text{конф}}$. В обоих случаях формулы метода анализа иерархий могут быть заменены формулой $t = \frac{1}{1+r'} t^{\text{цел}} + \frac{r'}{1+r'} t^{\text{конф}}$ где r' - параметр, характеризующий во сколько раз решение, принимаемое политикой конфиденциальности, более значимо, чем решение политики целостности.

3. Применение метода анализа иерархий дает наиболее значимые результаты в случае, когда $t^{\text{конф}}$ и $t^{\text{цел}}$ имеют разные знаки и $((r_1 > 1) \wedge (r_2 < 1)) \vee ((r_1 < 1) \wedge (r_2 > 1))$.

Таблица 2: Матрицы парных сравнений

t'	Цел.	Конф.
Цел.	1	$1/x$
Конф.	x	1

цел.	ДПБ.	МПБ.
ДПБ.	1	$1/x_1$
МПБ.	x_1	1

конф.	ДПБ.	МПБ.
ДПБ.	1	$1/x_2$
МПБ.	x_2	1

Существует возможность предложить другой вариант дерева решения метода анализа иерархий: вершина иерархии - уровень разрешения t'; критерии: политика целостности и политика конфиденциальности; альтернативы: ДПБ и МПБ - дискреционная и мандатная политики безопасности.

Пусть решение, принимаемое политикой конфиденциальности, в x раз более значимо, чем решение политики целостности. Предпочтительность мандатной модели разграничения доступа по сравнению с дискреционной оценивается двумя параметрами: x_1 - для политики целостности, x_2 - для политики конфиденциальности. Тогда матрицы парных сравнений задаются таблицей 2.

Формулы для вычисления относительных приоритетов дискреционной и мандатной политик безопасности принимают следующий вид:

$$X_{\text{ДПБ}} = \frac{1}{1+x_1} \times \frac{1}{1+x} + \frac{1}{1+x_2} \times \frac{x}{1+x}, X_{\text{МПБ}} = \frac{x_1}{1+x_1} \times \frac{1}{1+x} + \frac{x_2}{1+x_2} \times \frac{x}{1+x} = 1 - X_{\text{ДПБ}}. \quad (8)$$

Окончательное решение о предоставлении доступа теперь может быть вычислено по формулам:

$$t' = X_{\text{ДПБ}} \times t'_{\text{ДПБ}} + X_{\text{МПБ}} \times t'_{\text{МПБ}}, t'_{\text{ДПБ}} = \frac{1}{1+x} t^{\text{цел}}_{\text{ДПБ}} + \frac{x}{1+x} t^{\text{конф}}_{\text{ДПБ}}, t'_{\text{МПБ}} = \frac{1}{1+x} t^{\text{цел}}_{\text{МПБ}} + \frac{x}{1+x} t^{\text{конф}}_{\text{МПБ}}. \quad (9)$$

Используя представленные ранее формулы для вычисления уровней разрешения t и t', несложно доказать следующую теорему.

Теорема 1. *Если* $r = x1 = x2$ *и* $r1 = r2 = x$, *то* $t = t'$.

Таким образом, в случае совпадения приоритетов в разрезе выбранной модели разграничения доступа и в разрезе политик конфиденциальности и целостности, оба подхода к построению дерева решения МАИ приводят к одному и тому же уровню разрешения. В конечном итоге, выбор дерева решения зависит от порядка администрирования, определенного в системе.

Заключение

Предложенный подход, реализующий единую политику безопасности, по ряду характеристик превосходит традиционный подход, который заключается в требовании одновременного разрешения доступа всеми действующими в системе политиками безопасности. Наличие весовых коэффициентов, уровней разрешений позволяет администратору достаточно гибко настраивать уровни влияния различных правил безопасности. Использование двух политик безопасности с различными принципами имеет смысл, если их действие направлено на предотвращение угроз, связанных с различными каналы утечки информации. Поэтому выбор весовых коэффициентов при использовании алгоритма принятия решений необходимо осуществлять на основе анализа вероятности осуществления различных атак.

Следует обратить внимание на тот факт, что необходимость принятия решения о доминировании одной политики безопасности над другой возникает только в случае противоречий разрешений по одному и тому же запросу на доступ. С одной стороны, в системах, допускающих непротиворечивое администрирование безопасности, таких конфликтов не возникает. С другой стороны, если между двумя политиками безопасности никогда не возникает противоречий, то одну из политик безопасности можно отключить без ущерба защищенности системы.

Предложенный подход может найти применение в проектировании дополнительных систем защиты информации, а также в программных комплексах с собственной подсистемой безопасности.

Список литературы

[1] S.V. Belim, N.F. Bogachenko, J.S. Rakitsky Theoretical-Graph Approach to the Problem of Combining Role-Based and Mandatory Security Policies. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2:9–17, June 2010.

[2] S.V. Belim, N.F. Bogachenko, J.S. Rakitsky Combining of Role-Based and Mandatory Security Policies. *Problemy obrabotki i zashchity informatsii. Kniga 1. Modeli politik bezopasnosti komp'iuternykh sistem. Kollektivnaia monografiia* , 117–132, 2010.

[3] K.A. Shcheglov, A.Yu. Shcheglov New Approach to Data Securing in Information System. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie*, 58(3):157–166, 2015.

[4] M. Bishop *Applying the Take-Grant Protection Model. Technical Report.* Dartmouth College Hanover, NH, USA, 1990.

[5] URL: `https://scholar.google.co.uk/citations?view_op=view_citation&hl=ru&user=3PHaUacAAAAJ&citation_for_view=3PHaUacAAAAJ:LPZeul_q3PIC`.

[6] URL: `http://ocean.otr.usm.edu/~w300778/is-doctor/pubpdf/sc2008.pdf`.

[7] M.M. Kocat?rk, T.I. G?ndema Fine-Grained Access Control System Combining MAC and RBAC Models for XML. *Informatica*, 19(4):517–534, 2008.

[8] N.F. Bogachenko, S.V. Belim, S.Yu. Belim Using Analytic Hierarchy Process for Building of Role Based Access Control. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 3:7–17, 2013.

[9] S.V. Belim, N.F. Bogachenko Using a Hierarchy Analysis Method to Assess Permission Leakage Risks in Systems with a Role Based Access Control. *Informatsionno-upravliaiushchie sistemy*, 6:67–72, 2013.

[10] S.V. Belim, S.Yu. Belim, N.F. Bogachenko Creation of Role-Base Access Control with Use of Analytic Hierarchy Process. *Problemy obrabotki i zashchity informatsii. Kniga 4. Algoritmy zashchity dannykh*, 7–47, 2015.

Algorithms of Decision Support as a Way of Joint Different Security Policies

Nadezda F. Bogachenko, Yuriy S. Rakitskiy

The problem of joint implementation of several security policies in one information environment is topical issue of computer system administrating. The requirement of existence of at least two security policies is available in the modern standards of information security in automated systems. The majority of the offered methods of the solution of the task of joint implementation of security policies are reduced to search of the ideal decision in which settings of all shared security policies don't contradict each other. In practice it isn't always possible to find such settings, besides the fact of existence of the ideal decision isn't proved. The approach based on decision support algorithms is one of perspective solutions of the delivered problem.