УДК 004.056
doi:10.15217/issn1684-8853.2016.5.66

СОВМЕЩЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ, ОСНОВАННОЕ НА АЛГОРИТМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

С. В. Белим[a], *доктор физ.-мат. наук, профессор*
Н. Ф. Богаченко[a], *канд. физ.-мат. наук, доцент*
Ю. С. Ракицкий[a], *канд. техн. наук, доцент*
[a]*Омский государственный университет им. Ф. М. Достоевского, Омск, РФ*

Введение: *проблема совмещения нескольких политик безопасности в одной информационной среде является актуальной задачей администрирования компьютерных систем. Современные стандарты защиты информации в автоматизированных системах требуют наличия как минимум двух политик безопасности. Большинство предлагаемых методов решения задачи совмещения политик безопасности сводится к поиску идеального подхода, при котором настройки всех совместно используемых политик безопасности не противоречат друг другу. На практике не всегда удается найти такие настройки, кроме того, отсутствует доказательство самого факта существования идеального подхода. Одним из перспективных путей поиска ответов на поставленные вопросы является методика, основанная на алгоритмах поддержки принятия решений.* ***Результаты:*** *предложен алгоритм совмещения нескольких политик безопасности, который для каждого запроса на доступ принимает решение о том, какая политика безопасности будет задействована. Алгоритм использует взвешенную сумму уровней разрешения отдельных политик безопасности и метод анализа иерархий. Представлены формулы расчета уровня разрешения запрашиваемого доступа для дискреционной и мандатной политик безопасности. В дискреционной политике уровень разрешения запрашиваемого доступа определяется такими числовыми характеристиками, как общее число разрешенных прав доступа, число запрашиваемых прав доступа, число запрещенных прав доступа. Для мандатной политики вычисление уровня разрешения запрашиваемого доступа зависит от типа используемой решетки ценностей. Метод анализа иерархий находит свое применение, когда в системе действует две пары политик безопасности: одна связана с конфиденциальностью, другая — с целостностью. Предложено два дерева решения метода анализа иерархий для расчета итогового уровня разрешения запрашиваемого доступа.* ***Практическая значимость:*** *наличие весовых коэффициентов в предложенном алгоритме совмещения нескольких политик безопасности позволяет осуществлять настройку степени влияния тех или иных правил безопасности для перекрытия различных каналов утечки информации. Представленный подход может быть полезен при построении информационных систем с собственной подсистемой безопасности и проектировании дополнительных систем защиты информации.*

Ключевые слова *— совмещение политик безопасности, уровень разрешения, алгоритм принятия решений, метод анализа иерархий.*

Введение

Проблема совмещения различных политик безопасности возникает достаточно часто при администрировании компьютерных систем. Стандарты защиты информации в автоматизированных системах подразумевают наличие более одной политики разграничения доступа. Так, в «Оранжевой книге» использование только дискреционного разделения доступа относит компьютерную систему к одному из классов безопасности группы «С», тогда как добавление мандатного контроля доступа позволяет претендовать на более высокий класс защищенности группы «В». Причем «Оранжевой книгой» подразумевается именно добавление мандатной политики безопасности (МПБ) с сохранением возможностей дискреционной политики безопасности (ДПБ). В качестве еще одного примера совмещения политик безопасности можно привести системы управления базами данных, функционирующие на базе операционных систем семейства Windows. В системах управления базами данных наиболее распространенной является ролевая политика безопасности, но при этом данные хранятся в файлах, доступ к которым разграничивается операционной системой. В операционных системах базовой является ДПБ, но при этом реализуется на определенном уровне МПБ. Таким образом, требуется сопряжение трех различных политик безопасности.

Стандартным подходом является поиск идеального решения, при котором настройки одной политики безопасности не противоречат настройкам другой политики безопасности. В настоящее время предложен ряд различных решений. Работы [1, 2] посвящены совместной реализации ролевой и мандатной концепций разграничения доступа. Теоретико-графовый подход к решетке ценностей МПБ позволил совместить требования на орграф сущностей компьютерной системы и со стороны ролевой, и со стороны мандатной моделей. Предложен алгоритм создания политики безопасности, включающей в себя мандатное и ролевое разграничения доступа. Авторы работы [3] предлагают изменить базовые координаты матрицы доступов: правила доступа устанавливаются не между субъектом и объектом,

а между «субъектом доступа, запрашивающим доступ к объекту», и «субъектом доступа, создавшим этот объект». Показано, что такой подход позволяет дискреционный и мандатный механизмы контроля доступа использовать совместно. В работе [4] рассмотрено расширение дискреционной модели Take-Grant, учитывающее механизм мандатного разграничения доступа. В статье [5] предложен универсальный язык, позволяющий описать и реализовать глобальную комплексную политику безопасности для системы, состоящей из различных информационных сред, каждая из которых имеет собственную модель обеспечения безопасности и домен администрирования. Этот язык реализуется монитором событий. Конфликты между политиками безопасности разрешаются путем явного вызова администратора для принятия приоритетного решения. В работе [6] матрицу доступов ДПБ 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, оставаясь в рамках ДПБ. В работе [7] представлена модель управления доступом для работы с XML-документами. В этой модели комбинируются 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.

Однако есть принципиальная проблема реализации идеального подхода, состоящая в отсутствии доказательства того, что идеальное решение существует. Более того, практическая реализация одновременного администрирования нескольких политик безопасности показывает, что не всегда удается добиться настроек, обеспечивающих правильное функционирование системы. Данная статья посвящена новому подходу к совмещению нескольких политик безопасности в одной компьютерной системе, основанному на алгоритмах поддержки принятия решений.

Постановка задачи и общий подход к решению

Рассмотрим систему, в которой одновременно реализованы дискреционная и мандатная политики безопасности. Согласно общепринятому мнению, которое получило воплощение практически во всех стандартах информационной безопасности, МПБ обеспечивает более высокий уровень защиты информации и доминирует над ДПБ, которая обеспечивает базовый уровень защиты данных. При возникновении противоречий между настройками двух политик безопасности традиционно используется два подхода. Согласно первому подходу доступ запрещен, если он запрещен хотя бы одной политикой безопасности. Во втором случае МПБ занимает доминирующее положение, и решение о разрешении доступа принимается исходя из ее настроек. Первый подход легко приводит к полной неработоспособности системы, второй — практически к выключению ДПБ. Более того, МПБ ориентирована на систему в целом. Администратор определяет метки безопасности субъектов и объектов системы, которые могут изменяться только при смене состояния системы в целом, но не в отдельно взятом доступе. Тем не менее возможны исключительные ситуации. Например, администратору необходимо разрешить доступ конкретного субъекта к конкретному объекту, противоречащий МПБ. Администратор следит за содержимым объекта и может гарантировать отсутствие утечки информации через данный субъект, но не может дать гарантии отсутствия утечки через другие субъекты с тем же уровнем доступа. Данное разрешение может быть реализовано с помощью введения некоторых дополнительных меток безопасности для каждого конкретного случая, что приводит к существенному увеличению и запутыванию решетки ценностей и, как следствие, усложнению администрирования системы. Другой подход состоит в привлечении ДПБ, которая в одном заданном случае должна доминировать над МПБ. Другими словами, в системе может быть реализована надстройка, которая принимает решение о доминировании той или иной политики безопасности в каждом конкретном случае.

Сформулируем постановку задачи более строго. Пусть в системе действует две политики безопасности, которые принимают решения на основе алгоритмов S_1 и S_2. Необходимо реализовать алгоритм S, который для каждого запроса на доступ будет принимать решение о том, какая политика безопасности будет задействована. Следует отметить, что использование алгоритма S действительно необходимо только в том случае, когда решения, принимаемые S_1 и S_2, противоречат друг другу.

Традиционно в рамках политики безопасности на запрос о доступе принимается решение из множества $\{0, 1\}$, в котором нулевое значение соответствует отказу в доступе, а единичное — разрешению доступа. Для принятия решения о возможности доступа расширим область значений алгоритма принятия решения заданной политики безопасности 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 уровень доверия к доступу. Таким образом, уровень разрешения можно связать с вероятностью утечки информации при заданном доступе: чем выше вероятность p, тем меньше должен быть уровень разрешения t. С другой стороны, количественная оценка уровня разрешения t — это в некотором роде априорная информация о возможности утечки информации при запрашиваемом доступе. В первом приближении $p = 0{,}5 - (t \,/\, 2T)$.

При изложенном подходе решение о предоставлении доступа той или иной политикой безопасности (тем или иным алгоритмом) сводится к вычислению 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:

$$t = \frac{r}{r+1} t_1 + \frac{1}{r+1} t_2. \qquad (1)$$

Равнозначность политик безопасности достигается при $r = 1$. Следует отметить, что t не обязательно является целым числом: $t \in [-T, T]$.

Совмещение мандатной и дискреционной политик безопасности

Рассмотрим наиболее распространенный случай совмещения мандатной и дискреционной политик безопасности.

Для МПБ ограничимся простейшим вариантом линейной решетки ценностей с L уровнями безопасности. Тогда уровень разрешения может быть найден как разность между уровнем доверия субъекта $C(S)$ и уровнем секретности объекта $C(O)$:

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

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

Для ДПБ уровень разрешения может устанавливаться произвольно администратором для каждого доступа. Если администратор хочет присвоить доступу высший приоритет, то он назначает $t_2 = T$. Поэтому ограничимся случаем назначения уровня разрешения по умолчанию. Будем считать, что общее количество возможных видов доступа равно M. Пусть субъект запрашивает доступ к объекту по нескольким видам доступа. В случае запрета доступа будем считать, что

$$t_2 = -k \frac{T}{M}, \qquad (3)$$

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

$$t_2 = h \frac{T}{M}, \qquad (4)$$

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

Пример 1. Рассмотрим модельный пример функционирования такой системы. Положим $T = 4$. Пусть МПБ строится на основе линейной решетки ценностей с пятью уровнями: $SL = \{0, 1, 2, 3, 4\}$. Для ДПБ определены четыре вида доступа: $R = \{r, w, a, f\}$. В некоторый момент времени поступает запрос на доступ (S, O, r), которому в матрице доступов соответствует ячейка $\mathbf{M}[S, O] = \{r, w, a\}$, уровень секретности объекта $C(O) = 2$, уровень доверия субъекта $C(S) = 1$. В этом случае $t_1 = C(S) - C(O) = -1$, $t_2 = 2$. При равноправии политик безопасности по формуле (1) получаем $t = 1/2 > 0$, т. е. доступ разрешен, несмотря на запрет МПБ. Если же повысить приоритет МПБ в 3 раза, согласно формуле (1): $t = -1/4 < 0$. В этом случае доступ будет запрещен.

При совмещении мандатной и дискреционной политик безопасности был рассмотрен простейший случай линейной решетки ценностей. Однако в реальных системах МПБ 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 МПБ.

Классическая модель МПБ определяет оператор $\sup(\cdot,\cdot)$, 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 $\mathrm{dif}(\cdot,\cdot)$, показывающий «расстояние» от уровня безопасности l_1 до наименьшей верхней границы уровней безопасности l_1, l_2: $\mathrm{dif}(l_1, \sup(l_1, l_2)) = \sup(l_1, l_2) - l_1$. Такой подход возможен, поскольку элементы решетки l_1 и $\sup(l_1, l_2)$ будут всегда сравнимы по определению. Данный оператор позволяет определить количе-

ство 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 $\sup(C(S), C(O))$:

$$t_1 = -1 \cdot \left| \left(\mathrm{dif}\left(C(S), \sup\left(C(S), C(O)\right)\right) - \right.\right. \\ \left.\left. - \mathrm{dif}\left(C(O), \sup\left(C(S), C(O)\right)\right)\right)\right| \frac{T}{H}, \quad (5)$$

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

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.

Пример 2. Пусть МПБ строится на основе нелинейной решетки ценностей с восемью уровнями секретности: $SX = \{0, 1a, 1b, 1c, 2ab, 2c, 3, 4\}$. При этом $0 \le 1a$, $0 \le 1b$, $0 \le 1c$ (уровни $1a$, $1b$, $1c$ несравнимы), $1a \le 2ab$, $1b \le 2ab$, $1c \le 2c$ (уровни $2ab$, $2c$ несравнимы), $2ab \le 3$, $2c \le 3$, $3 \le 4$. Несложно проверить, что $H = 3$. Пусть поступает запрос на доступ субъекта S к объекту O, $C(O) = 1c$, $C(S) = 2ab$. В этом случае $\sup(C(S), C(O)) = 3$, $\mathrm{dif}(C(S), \sup(C(S), C(O))) = 1$, $\mathrm{dif}(C(O), \sup(C(S), C(O))) = 2$. При $T = 3$ по формуле (5) получаем $t_1 = -1 \cdot |1 - 2| = -1$.

Обобщая предложенные правила вычисления уровней разрешения, приведем схему алгоритма S, который для каждого запроса на доступ принимает решение о предоставлении доступа на основе решений мандатной и дискреционной политик безопасности.

1. Вычислить уровень разрешения МПБ t_1:

1.1) если МПБ строится на основе линейной решетки ценностей, для расчета t_1 применить формулу (2);

1.2) иначе решетка ценностей МПБ является нелинейной, для расчета t_1 применить формулу (5).

2. Уровень разрешения ДПБ t_2 назначить по умолчанию в соответствии с матрицей доступов:

2.1) если доступ запрещен, для расчета t_2 применить формулу (3);

2.2) иначе доступ разрешен, для расчета t_2 применить формулу (4).

3. Принять решение о предоставлении доступа:

3.1) если $t_1 < 0$ и $t_2 < 0$, то доступ запретить;

3.2) иначе, если $t_1 \ge 0$ и $t_2 \ge 0$, то доступ разрешить;

3.3) иначе вычислить обобщенный уровень разрешения t по формуле (1). Если $t < 0$, то доступ запретить, иначе — доступ разрешить.

Применение метода анализа иерархий

Часто в одной системе действует по две мандатные и дискреционные политики безопасности: одна пара связана с конфиденциальностью, другая — с целостностью. В этом случае для вычисления уровня разрешения удобнее воспользоваться методом анализа иерархий (МАИ) 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 МАИ неоднократно применялся для решения задач информационной безопасности, в частности, в статьях [8–10] метод был использован для построения модели ролевого разграничения доступа.

Согласно МАИ, необходимо заполнить три матрицы парных сравнений: одна — для уровня критериев и две — для уровня альтернатив. Пусть, как и ранее, r ($r > 0$) — коэффициент доминирования, показывающий, во сколько раз решение, принимаемое МПБ, более значимо, чем решение ДПБ. Предпочтительность политики конфиденциальности по сравнению с политикой целостности оценивается двумя подобными параметрами: r_1 ($r_1 > 0$) — для дискреционной модели, r_2 ($r_2 > 0$) — для мандатной модели. Тогда матрицы парных сравнений задаются табл. 1.

Идеальная согласованность этих матриц следует из того факта, что для двумерной обратно симметричной матрицы **M** всегда выполняется условие: $\forall i, j, k$ имеет место равенство

■ ***Таблица 1***

t	ДПБ	МПБ
ДПБ	1	$1/r$
МПБ	r	1

ДПБ	цел.[1]	конф.[2]
цел.	1	$1/r_1$
конф.	r_1	1

МБП	цел.	конф.
цел.	1	$1/r_2$
конф.	r_2	1

[1] цел. — целостность.

[2] конф. — конфиденциальность.

$[\mathbf{M}]_{ij} = [\mathbf{M}]_{ik} \times [\mathbf{M}]_{kj}$. В этом случае относительные весовые коэффициенты определяются нормированными столбцами (например, первыми) всех трех матриц парных сравнений, а формулы для вычисления относительных приоритетов политики целостности и политики конфиденциальности принимают следующий вид:

$$R^{\text{цел}} = \frac{1}{1+r_1}\frac{1}{1+r} + \frac{1}{1+r_2}\frac{r}{1+r};$$

$$R^{\text{конф}} = \frac{r_1}{1+r_1}\frac{1}{1+r} + \frac{r_2}{1+r_2}\frac{r}{1+r} = 1 - R^{\text{цел}}.$$

Окончательное решение о предоставлении доступа теперь может быть вычислено по формулам

$$t = R^{\text{цел}} t^{\text{цел}} + R^{\text{конф}} t^{\text{конф}},$$

$$t^{\text{цел}} = \frac{1}{1+r} t^{\text{цел}}_{\text{ДПБ}} + \frac{r}{1+r} t^{\text{цел}}_{\text{МПБ}},$$

$$t^{\text{конф}} = \frac{1}{1+r} t^{\text{конф}}_{\text{ДПБ}} + \frac{r}{1+r} t^{\text{конф}}_{\text{МПБ}},$$

где верхний индекс означает политику конфиденциальности или целостности, а нижний — дискреционное или мандатное разграничение доступа. Пары величин $t^{\text{цел}}_{\text{ДПБ}}$ и $t^{\text{цел}}_{\text{МПБ}}$, 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 предыдущем разделе. Анализируя полученные формулы, можно сделать следующие выводы.

1. Так как $R^{\text{цел}}$ и $R^{\text{конф}}$ принадлежат интервалу (0, 1), то применение МАИ 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 МАИ 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 МАИ дает наиболее интересные результаты в ситуации, когда $t^{\text{конф}}$ и $t^{\text{цел}}$ имеют разные знаки и $((r_1 > 1) \wedge (r_2 < 1)) \vee ((r_1 < 1) \wedge (r_2 > 1))$.

Пример 3. Пусть $t^{\text{цел}}_{\text{ДПБ}} = 3$, $t^{\text{цел}}_{\text{МПБ}} = -1$, $t^{\text{конф}}_{\text{ДПБ}} = 2$, $t^{\text{конф}}_{\text{МПБ}} = -2$. Положим $r = 2$. Тогда $t^{\text{цел}} = 1/3$, $t^{\text{конф}} = -2/3$. Очевидно, что для разрешения доступа необходимо потребовать, чтобы предпочтительность политики конфиденциальности (r_i) для одной из моделей разграничения доступа была меньше предпочтительности политики целостности ($1/r_j$) для другой модели. Пусть $r_1 = 2$, $r_2 = 1/3$, тогда $R^{\text{цел}} = 11/18$, $R^{\text{конф}} = 7/18$, $t = -1/18 < 0$. Таким образом, доступ будет запрещен, приоритет получит политика конфиденциальности. Если же $r_1 = 1$, $r_2 = 1/5$, тогда $R^{\text{цел}} = 13/18$, $R^{\text{конф}} = 5/18$, $t = 1/6 > 0$. Доступ будет разрешен, и приоритет получит политика целостности.

Рассмотрим далее другой вариант дерева решения МАИ: вершина иерархии — уровень разрешения $\hat{t}$; 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 табл. 2.

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

$$X_{\text{ДПБ}} = \frac{1}{1+x_1}\frac{1}{1+x} + \frac{1}{1+x_2}\frac{x}{1+x};$$

$$X_{\text{МПБ}} = \frac{x_1}{1+x_1}\frac{1}{1+x} + \frac{x_2}{1+x_2}\frac{x}{1+x} = 1 - X_{\text{ДПБ}}.$$

Окончательное решение о предоставлении доступа теперь может быть вычислено по формулам

$$\hat{t} = X_{\text{ДПБ}} \hat{t}_{\text{ДПБ}} + X_{\text{МПБ}} \hat{t}_{\text{МПБ}},$$

$$\hat{t}_{\text{ДПБ}} = \frac{1}{1+x} t^{\text{цел}}_{\text{ДПБ}} + \frac{x}{1+x} t^{\text{конф}}_{\text{ДПБ}},$$

$$\hat{t}_{\text{МПБ}} = \frac{1}{1+x} t^{\text{цел}}_{\text{МПБ}} + \frac{x}{1+x} t^{\text{конф}}_{\text{МПБ}}.$$

Пример 4. Пусть, как и прежде, $t^{\text{цел}}_{\text{ДПБ}} = 3$, $t^{\text{конф}}_{\text{ДПБ}} = 2$, $t^{\text{цел}}_{\text{МПБ}} = -1$, $t^{\text{конф}}_{\text{МПБ}} = -2$. Положим $x = 3$. Тогда $\hat{t}_{\text{ДПБ}} = 9/4$, $\hat{t}_{\text{МПБ}} = -7/4$. Пусть $x_1 = 1$, $x_2 = 1/3$, тогда $X_{\text{ДПБ}} = 11/16$, $X_{\text{МПБ}} = 5/16$, $\hat{t} = 1 > 0$. Таким образом, доступ будет разрешен, приоритет получит ДПБ. Если же $x_1 = 1/2$, $x_2 = 2$, тогда

■ *Таблица 2*

$\hat{t}$	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

$X_{ДПБ} = 5/12$, $X_{МПБ} = 7/12$, $\hat{t} = -1/12 < 0$. Доступ будет запрещен, и приоритет получит МПБ.

Используя представленные ранее формулы для вычисления уровней разрешения t и $\hat{t}$, несложно доказать следующее **утверждение:**

$$\text{если } r = x_1 = x_2 \text{ и } r_1 = r_2 = x, \text{ то } t = \hat{t}.$$

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 к построению единой политики безопасности обладает рядом преимуществ по сравнению с традиционным требованием одновременного разрешения доступа всеми активными политиками безопасности. Наличие весовых коэффициентов позволяет администратору достаточно гибко настраивать степени влияния различных правил безопасности. Использование двух различных по типу политик безопасности имеет смысл, если они перекрывают различные каналы утечки информации. В связи с этим выбор весовых коэффициентов в алгоритме принятия решений необходимо осуществлять на основе анализа вероятности различных атак.

Следует подчеркнуть, 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.

Литература

1. **Белим С. В., Богаченко Н. Ф., Ракицкий Ю. С.** Теоретико-графовый подход к проблеме совмещения ролевой и мандатной политик безопасности // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 9–17.
2. **Белим С. В., Богаченко Н. Ф., Ракицкий Ю. С.** Совмещение ролевой и мандатной политик безопасности // Проблемы обработки и защиты информации. Кн. 1: Модели политик безопасности компьютерных систем: Коллективная монография. — Омск: Полиграфический центр КАН, 2010. — С. 117–132.
3. **Щеглов К. А., Щеглов А. Ю.** Новый подход к защите данных в информационной системе // Известия высших учебных заведений. Приборостроение. 2015. Т. 58. № 3. С. 157–166.
4. **Bishop M.** Applying the Take-Grant Protection Model. Technical Report. — Dartmouth College Hanover, NH, USA, 1990. — 26 p.
5. **Ribeiro C., Zuquete A., Ferreira P., Guedes P.** SPL: An Access Control Language for Security Policies with Complex Constraints // Proc. of the Network and Distributed System Security Symposium. Sun Diego, CA. 2001. https://scholar.google.co.uk/citations?view_op=view_citation&hl=ru&user=3PHaUacAAAAJ&citation_for_view=3PHaUacAAAAJ:LPZeul_q3PIC (дата обращения: 18.07.2016).
6. **Lunsford D. L., Collins M. R.** The CRUD Security Matrix: A Technique for Documenting Access Rights // Proc. of the 7th Annual Security Conf. Las Vegas, NV, 2008. http://ocean.otr.usm.edu/~w300778/is-doctor/pubpdf/sc2008.pdf (дата обращения: 18.07.2016).
7. **Kocatürk M. M., Gündema T. I.** Fine-Grained Access Control System Combining MAC and RBAC Models for XML // Informatica. 2008. Vol. 19. Iss. 4. P. 517–534.
8. **Богаченко Н. Ф., Белим С. В., Белим С. Ю.** Использование метода анализа иерархий для построения ролевой политики безопасности // Проблемы информационной безопасности. Компьютерные системы. 2013. № 3. С. 7–17.
9. **Белим С. В., Богаченко Н. Ф.** Применение метода анализа иерархий для оценки рисков утечки полномочий в системах с ролевым разграничением доступа // Информационно-управляющие системы. 2013. № 6. С. 67–72.
10. **Белим С. В., Белим С. Ю., Богаченко Н. Ф.** Построение ролевого разграничения доступа с использованием метода анализа иерархий // Проблемы обработки и защиты информации. Кн. 4: Алгоритмы защиты данных. — Омск: Изд-во Омского гос. ун-та, 2015. — С. 7–47.

UDC 004.056
doi:10.15217/issn1684-8853.2016.5.66

The Security Policies Joint Implementation Based on Decision Support Algorithms

Belim S.V.[a], Dr. Sc., Phis.-Math., Professor, sbelim@mail.ru
Bogachenko N. F.[a], PhD, Phis.-Math., Associate Professor, nfbogachenko@mail.ru
Rakitskiy Yu. S.[a], PhD, Tech., Associate Professor, yrakitsky@gmail.com
[a]Dostoevsky Omsk State University, 55, A, Mira St., 644077, Omsk, Russian Federation

Introduction: The problem of joint implementation of several security policies in one information environment is a topical issue in computer system administrating. The modern standards of information security in automated systems requre that at least two security policies are available. Most of the offered methods to solve the joint implementation problem can be reduced to the search for an ideal solution when the settings of all the shared security policies do not contradict each other. In practice, it is not always possible to find such settings, and the very existence of an ideal solution is not proved. An approach based on decision-making support algorithms is a promising way to find answers to these questions. **Results:** An algorithm of combining several security policies is offered. For each request for access, it makes a decision on what security policy will be involved. This algorithm uses a weighed sum of permission levels for separate security policies, and the Analytic Hierarchy Process. Formulas are presented to calculate the permission level of the required access for the discretionary and mandatory security policies. In the discretionary security policy, the permission level of a required access is defined by such numerical characteristics as the total number of the allowed access rights, the number of the required access rights, and the number of the forbidden access rights. For the mandatory security policy, the calculation of the permission level of a required access depends on the type of the security lattice. The analytic hierarchy process finds application when two couples of security policies work in the system, one couple related to confidentiality, an the other one related to integrity. Two solution trees are offered for analytic hierarchy process to calculate the total permission level of the required access. **Practical relevance:** The algorithm proposed for joint implementation of security policies contains weight factors. This allows us to set up the level of influence for different security rules so that various channels of information leakage overlap. The proposed approach can be useful in building information systems with their own security subsystems, or in the development of extra systems of information security.

Keywords — Joint Implementation of Security Policies, Permission Level, Decision-Making Support Algorithms, Analytic Hierarchy Process.

References

1. Belim S. V., Bogachenko N. F., Rakitsky J. S. Theoretical-Graph Approach to the Problem of Combining Role-Based and Mandatory Security Policies. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2010, no. 2, pp. 9–17 (In Russian).
2. Belim S. V., Bogachenko N. F., Rakitsky J. S. Combining of Role-Based and Mandatory Security Policies. In: *Problemy obrabotki i zashchity informatsii. Kniga 1. Modeli politik bezopasnosti komp'iuternykh sistem* [Problems of Information Processing and Security. Book 1. Models of Security Policies of Computer Systems]. Omsk, Poligraficheskii tsentr KAN Publ., 2010, pp. 117–132 (In Russian).
3. Shcheglov K. A., Shcheglov A. Yu. New Approach to Data Securing in Information System. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie*, 2015, vol. 58, no. 3, pp. 157–166 (In Russian).
4. Bishop M. *Applying the Take-Grant Protection Model. Technical Report*. Dartmouth College Hanover, NH, USA, 1990. 26 p.
5. Ribeiro C., Zuquete A., Ferreira P., Guedes P. SPL: An Access Control Language for Security Policies with Complex Constraints. *Proc. of the Network and Distributed System Security Symp.*, Sun Diego, CA, 2001. Available at: https://scholar.google.co.uk/citations?view_op=view_citation&hl=ru&user=3PHaUacAAAAJ&citation_for_view=3PHaUacAAAAJ:LPZeul_q3PIC (accessed 18 July 2016).
6. Lunsford D. L., Collins M. R. The CRUD Security Matrix: A Technique for Documenting Access Rights. *Proc. of the 7th Annual Security Conf.*, Las Vegas, NV, 2008. Available at: http://ocean.otr.usm.edu/~w300778/is-doctor/pubpdf/sc2008.pdf (accessed 18 July 2016).
7. Kocatürk M. M., Gündema T. I. Fine-Grained Access Control System Combining MAC and RBAC Models for XML. *Informatica*, 2008, vol. 19, iss. 4, pp. 517–534.
8. Bogachenko N. F., Belim S. V., Belim S. Yu. Using Analytic Hierarchy Process for Building of Role Based Access Control. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2013, no. 3, pp. 7–17 (In Russian).
9. Belim S. V., Bogachenko N. F. Using a Hierarchy Analysis Method to Assess Permission Leakage Risks in Systems with a Role Based Access Control. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 6, pp. 67–72 (In Russian).
10. Belim S. V., Belim S. Yu., Bogachenko N. F. Creation of Role-Base Access Control with Use of Analytic Hierarchy Process. In: *Problemy obrabotki i zashchity informatsii. Kniga 4. Algoritmy zashchity dannykh* [Problems of Information Processing and Security. Book 4. Algorithms of Data Security]. Omsk, OmSU Publ., 2015, pp. 7–47 (In Russian).