# Об оценке ущерба от утечки полномочий в ролевой модели безопасности

С.В. Усов
raintower@mail.ru

Н.Ф. Богаченко
bogachenkonf@mail.ru

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

**Аннотация**

В данной работе предложен алгоритм оценки относительного ущерба от утечки полномочий в рамках ролевой модели разграничения доступа с иерархией на множестве ролей. Вычисление относительного ущерба производится по методу анализа иерархий. Приведена вариация алгоритма оценки относительного ущерба, не требующая привлечения экспертных оценок при использовании метода анализа иерархий. В такой вариации удается избежать систематических ошибок, присущих данному методу принятия решений.

## 1 Проблема утечки полномочий в иерархической ролевой модели безопасности

Ролевая модель разграничения доступа [1] базируется на идее разбиения множества субъектов на классы, называемые ролями, такие, что каждой роли приписывается определенный набор привилегий (или полномочий). Каждая привилегия, если подходить с точки зрения дискреционной политики безопасности, представляет собой предзаданный набор прав на определенные объекты. Пользователь получает соответствующий роли набор полномочий при авторизации на эту роль.

Развитие ролевой политики безопасности произведено в таких работах, как [2]. В рамках данной статьи мы будем основываться на построении ролевого разграничения доступа с использованием метода анализа иерархий [3], предложенного в [4].

Проблема утечки прав доступа – ключевая проблема в направлении изучения моделей безопасности компьютерных систем. В случае ролевой модели ее можно интерпретировать как проблему утечки полномочий или же ролей. В [4] предложена методика оценки вероятностей утечки полномочий. Таким образом, если удастся подсчитать ущерб, возникающий по причине утечки каждого из полномочий, можно оценить ущерб, причиняемый нарушением ролевой политики безопасности в целом.

В ролевой модели безопасности определяются $R = \{r_1, \ldots, r_n\}$ – множество всех ролей системы, и $P = \{p_1, \ldots, p_m\}$ – множество всех привилегий системы. Каждой роли сопоставлен определенный набор привилегий. На множестве ролей вводится частичный порядок, тем самым задается иерархия, которую можно представить в виде ориентированного графа (ациклического). Если роль $r$ находится в иерархии выше роли $r'$, то есть $r > r'$, то она обладает всеми привилегиями, которыми обладает роль $r'$. Иерархию будем представлять ориентированным деревом, в котором нелистовым вершинам соответствуют вспомогательные роли, листовым – роли конечных пользователей.



In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2017 (DMS-2017), Omsk, Russia, October 2017, published at http://ceur-ws.org

В [4] в рамках нескольких предположений, которые используются в качестве аналога экспертных оценок в методе анализа иерархий, оценивается риск утечки полномочий. Предположения следующие:

1. Чем больше полномочий содержит роль, тем выше вероятность атаки на нее.
2. Чем чаще встречается полномочие, тем выше вероятность его утечки.
3. Чем выше роль в иерархии, тем выше вероятность атаки на нее.

Считая вероятности утечки полномочий $P(p_1), \ldots, P(p_m)$ уже определенными по предложенному алгоритму [4], приступим к построению оценки ущерба.

## 2 Задача нахождения относительного ущерба от утечки полномочий

Будем решать следующую задачу. Пусть задана иерархия ролей системы, для каждой роли задан набор приписанных ей полномочий. Требуется рассчитать сравнительный ущерб от успешной атаки на каждую из ролей с учетом расположения ролей и приписанных им полномочий в иерархии. При этом ущерб от утечки полномочий может быть не задан даже в относительной форме.

При расчете ущерба будем использовать следующие эвристики:

1. Чем реже встречается привилегия в иерархии ролей, тем выше ущерб от ее утечки.
2. Чем реже встречается привилегия среди листовых ролей (которые назначаются конечным пользователям), тем выше ущерб от ее утечки, причем зависимость носит экспоненциальный характер.

Данные предположения основываются на том, что наиболее «ценные» полномочия, утечка которых может привести к серьезному ущербу для системы (организации), приписываются относительно небольшому количеству ролей, которые назначаются наиболее ответственным пользователям: администраторам, членам руководства или службы безопасности организации. Разумеется, не всегда такие допущения хорошо коррелируют с реальным положением дел, но в случае отсутствия какой-либо дополнительной информации следует признать их разумными.

Для расчета сравнительного ущерба будем использовать метод анализа иерархий, где на уровне критериев (в терминах теории принятия решений) находятся привилегии, а на уровне альтернатив – роли (см. рис. 1). Нашей задачей будет упорядочить роли по уменьшению среднего ущерба, возникающего при похищении ролей.

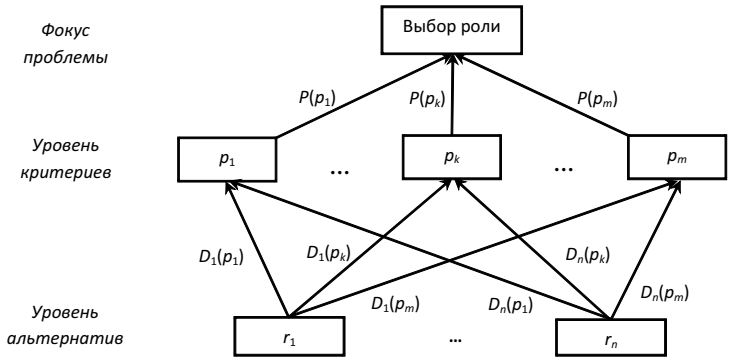


Рис. 1: Дерево решения метода анализа иерархий

Первая эвристика будет использоваться при составлении матриц парных сравнений для альтернатив, вторая – для вычисления определенных элементов этих матриц только в том случае, если ущерб от утечки полномочий не задан даже в относительной форме. Такой подход позволяет заполнить матрицы парных сравнений и решить задачу принятия решения без привлечения экспертов, что избавит полученное решение от влияния субъективных факторов.

С другой стороны, для учета индивидуальных характеристик системы с ролевым разграничением доступа сохраняется возможность высчитывать коэффициенты относительного ущерба для матриц парных сравнений не автоматически, а задавать их самостоятельно, или с привлечением экспертов. В этом случае вторая эвристика не применяется.

Относительные весовые коэффициенты $P(p_k)$ $(k = 1, \ldots, m)$ уровня критериев будем вычислять по предложенному в [4] алгоритму оценки рисков утечки полномочий.

Для расчета относительных весовых коэффициентов $D_i(p_k)$ $(i = 1, \ldots, n,\ k = 1, \ldots, m)$ уровня альтернатив используем метод парных сравнений. Матрицы $M^k$ парных сравнений альтернатив по $k$-му из

критериев (строки и столбцы соответствуют ролям системы) получим следующим образом: через $v_k$ обозначим отношение ущерба от утечки привилегии $p_k$ к стоимости ее обслуживания в условиях безопасности. Элементы матрицы $M^k$ вычисляем по следующему правилу:

$$M_{ij}^k = \begin{cases} v_k, & \text{если привилегия } p_k \text{ приписана к роли } r_i, \text{ но не приписана к роли } r_j, \\ \frac{1}{v_k}, & \text{если привилегия } p_k \text{ приписана к роли } r_j, \text{ но не приписана к роли } r_i, \\ 1, & \text{если привилегия } p_k \text{ приписана к обеим ролям } r_i \text{ и } r_j, \text{ либо не приписана ни к одной.} \end{cases} \quad (1)$$

Каждая такая матрица обладает свойствами матрицы парных сравнений, в частности, $M_{ii}^k = 1$. Более того, $M^k$ обладает идеальной согласованностью:

**Утверждение 1.** *Пусть матрица $M^k$ размера $n \times n$, где $n$ – количество ролей в системе, заполнена по правилу 1. Тогда $\forall i, j, l \in \{1 \dots n\}$ выполняется соотношение $M_{il}^k = M_{ij}^k \times M_{jl}^k$.*

Для доказательства этого утверждения достаточно проверить 8 случаев отношения привилегии $p_k$ к каждой из ролей $r_i$, $r_j$, $r_l$. Поскольку все случаи проверяются одинаково, ограничимся проверкой одного из них. Пусть $p_k$ относится к ролям $r_i$ и $r_l$, и не относится к $r_j$. Тогда $M_{ij}^k = v_k$, $M_{jl}^k = 1$, $M_{il}^k = \frac{1}{v_k}$, и действительно, $M_{il}^k = 1 = v_k \times \frac{1}{v_k} = M_{ij}^k \times M_{jl}^k$.

Поскольку матрица $M^k$ идеально согласована, столбцы нормированной матрицы $M^{k*}$ получатся одинаковыми. Таким образом, для вычисления весовых коэффициентов каждой альтернативы по $k$-му критерию достаточно выбрать и нормировать один (любой) столбец матрицы $M^k$. Мы будем использовать первый столбец, $(M^k)^1$, соответствующий роли $r_1$, находящейся в корне дерева иерархии ролей $T$. Поскольку роли $r_1$ приписаны все привилегии системы, в таком столбце могут стоять только единицы и $\frac{1}{v_k}$, причем единица на $i$-той позиции означает, что привилегия $p_k$ приписана роли $r_i$, а $\frac{1}{v_k}$ – что у роли $r_i$ привилегия $p_k$ отсутствует. На самом деле, конечно, удобнее перед нормированием домножить весь столбец $(M^k)^1$ на $v_k$, что мы и будем делать. Именно матрица, составленная из величин $w_i^k = M_{i1}^k \times v_k$, будет использоваться в алгоритме нахождения относительного ущерба.

Далее завершаем применение метода анализа иерархий, вычисляя сравнительные оценки ущерба для каждой роли по классической формуле МАИ [3].

В дальнейшем рассчитанные сравнительные оценки могут быть использованы, например, при решении задачи авторизации: какую роль (или набор ролей) следует назначить пользователю, чтобы он получил заданный набор привилегий? В качестве одного из критериев при выборе ролей предлагаем использовать минимизацию ущерба при злоупотреблении пользователем дополнительными полномочиями, которые достались ему вместе с назначенными ролями.

## 3 Алгоритм расчета относительного ущерба от утечки полномочий

Выпишем формально алгоритм расчета сравнительного ущерба от утечки полномочий. Пусть помеченное ориентированное дерево $T$, определяющее иерархию ролей, содержит $n$ вершин $r_1, \dots, r_n$ и пусть в системе определено $m$ полномочий $p_1, \dots, p_m$. Пусть для каждого полномочия $p_k$ рассчитана вероятность (риск) его утечки $P(p_k)$. Также для каждого полномочия $p_k$ задан коэффициент отношения ущерба от утечки этого полномочия к обслуживанию полномочия при безопасной работе $v_k$.

Заметим, что требование древовидности ролевой иерархии необходимо для расчета рисков утечки полномочий $P(p_k)$ по алгоритму, предложенному в [4]. Если эти величины получены каким-то иным способом, то ограничение на ролевую иерархию можно ослабить, потребовав лишь ацикличность.

Алгоритм по шагам можно записать в следующем виде.

Шаг 0. Если коэффициент $v_k$ не задан, для каждого полномочия $p_k$ назначить $v_k$ равным экспоненте отношения числа листовых ролей, не обладающих полномочием $p_k$, к числу ролей, обладающих полномочием $p_k$.

Шаг 1. Каждой вершине $r_i$ ролевого дерева $T$ поставить в соответствие величину $w_i^k$, равную $v_k$, если роли $r_i$ приписано полномочие $p_k$, и единице в противном случае.

Шаг 2. Для каждой роли $r_i$ и полномочия $p_k$ вычислить относительные весовые коэффициенты затрат $D_i(p_k)$ по формуле:

$$D_i(p_k) = \frac{w_i^k}{\sum_{j=1}^n w_j^k}.$$

Шаг 3. Для каждой роли $r_i$ посчитать значение $D(p_k)$ по формуле метода анализа иерархий:

$$D(r_i) = \sum_{k=1}^{m} P(p_k) D_i(p_k).$$

Шаг 4. Теперь можно выбрать роль с наименьшим значением оценки ущерба, либо расположить роли в порядке увеличения этой оценки.

**Утверждение 2.** *Трудоемкость алгоритма расчета сравнительного ущерба от утечки полномочий, основанного на методе анализа иерархий, равна* $\mathrm{O}(n \times m)$, *где* $n$ *– число ролей,* $m$ *– число полномочий в системе.*

## 4 Применение алгоритма расчета относительного ущерба от утечки полномочий

Рассмотрим применение предложенного алгоритма на примере иерархии ролей $T^1$, представленной на рис. 2. Пусть используется нестрогий таксономический подход к распределению полномочий, и полномочия

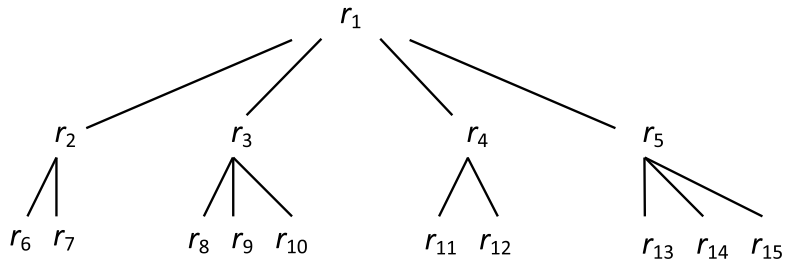


Рис. 2: Ролевое дерево $T^1$

листовых ролей имеют следующие значения: $r_6.p = \{p_1, p_2, p_3\}$, $r_7.p = \{p_2, p_4\}$, $r_8.p = \{p_3, p_4, p_5\}$, $r_9.p = \{p_3, p_5\}$, $r_{10}.p = \{p_2, p_4\}$, $r_{11}.p = \{p_2, p_5\}$, $r_{12}.p = \{p_1, p_4, p_5\}$, $r_{13}.p = \{p_3, p_5\}$, $r_{14}.p = \{p_1, p_2, p_5\}$, $r_{15}.p = \{p_5\}$. Для остальных ролей получаем полномочия из условия наследования: $r_2.p = \{p_1, p_2, p_3, p_4\}$, $r_3.p = \{p_2, p_3, p_4, p_5\}$, $r_4.p = \{p_1, p_2, p_4, p_5\}$, $r_5.p = \{p_1, p_2, p_3, p_5\}$, $r_1.p = \{p_1, p_2, p_3, p_4, p_5\}$.

Применяя алгоритм расчета рисков утечки полномочий [4], находим комбинированные весовые коэффициенты $P(p_k)$:

$P(p_1) \approx 0,14$, $P(p_2) \approx 0,23$, $P(p_3) \approx 0,16$, $P(p_4) \approx 0,17$, $P(p_5) \approx 0,30$.

Считая коэффициенты $v_k$ не заданными, рассчитаем их как экспоненту отношения числа листовых ролей, не обладающих полномочием $p_k$, к числу ролей, обладающих полномочием $p_k$:

$v_1 = e^{\frac{7}{3}}$, $v_2 = e^{\frac{5}{5}}$, $v_3 = e^{\frac{6}{4}}$, $v_4 = e^{\frac{6}{4}}$, $v_5 = e^{\frac{3}{7}}$.

Весовые коэффициенты $w_i^k$ занесем в матрицу $\mathbf{W}$, в которой $k$ будет индексировать столбец, а $i$ – строку.

$$\mathbf{W} = \begin{pmatrix}
e^{\frac{7}{3}} & e^{\frac{5}{5}} & e^{\frac{6}{4}} & e^{\frac{6}{4}} & e^{\frac{3}{7}} \\
e^{\frac{7}{3}} & e^{\frac{5}{5}} & e^{\frac{6}{4}} & e^{\frac{6}{4}} & 1 \\
1 & e^{\frac{5}{5}} & e^{\frac{6}{4}} & e^{\frac{6}{4}} & e^{\frac{3}{7}} \\
e^{\frac{7}{3}} & e^{\frac{5}{5}} & 1 & e^{\frac{6}{4}} & e^{\frac{3}{7}} \\
e^{\frac{7}{3}} & e^{\frac{5}{5}} & e^{\frac{6}{4}} & 1 & e^{\frac{3}{7}} \\
e^{\frac{7}{3}} & e^{\frac{5}{5}} & e^{\frac{6}{4}} & 1 & 1 \\
1 & e^{\frac{5}{5}} & 1 & e^{\frac{6}{4}} & 1 \\
1 & 1 & e^{\frac{6}{4}} & e^{\frac{6}{4}} & e^{\frac{3}{7}} \\
1 & 1 & e^{\frac{6}{4}} & 1 & e^{\frac{3}{7}} \\
1 & e^{\frac{5}{5}} & 1 & e^{\frac{6}{4}} & 1 \\
1 & e^{\frac{5}{5}} & 1 & 1 & e^{\frac{3}{7}} \\
e^{\frac{7}{3}} & 1 & 1 & e^{\frac{6}{4}} & e^{\frac{3}{7}} \\
1 & 1 & e^{\frac{6}{4}} & 1 & e^{\frac{3}{7}} \\
e^{\frac{7}{3}} & e^{\frac{5}{5}} & 1 & 1 & e^{\frac{3}{7}} \\
1 & 1 & 1 & 1 & e^{\frac{3}{7}}
\end{pmatrix}$$

Здесь, например, $w_4^3 = 1$, поскольку роли $r_4$ не приписано полномочие $p_3$, а $w_3^4 = v_4 = e^{\frac{6}{4}}$, поскольку роли $r_3$ приписано полномочие $p_4$.

Нормируем каждый столбец матрицы $\mathbf{W}$, тем самым получая матрицу $\mathbf{D}$, составленную из относительных весовых коэффициентов затрат $D_i(p_k)$, в которой $k$ будет индексировать столбец, а $i$ – строку.

$$\mathbf{D} = \begin{pmatrix} 0,129 & 0,084 & 0,105 & 0,105 & 0,073 \\ 0,129 & 0,084 & 0,105 & 0,105 & 0,048 \\ 0,012 & 0,084 & 0,105 & 0,105 & 0,073 \\ 0,129 & 0,084 & 0,023 & 0,105 & 0,073 \\ 0,129 & 0,084 & 0,105 & 0,023 & 0,073 \\ 0,129 & 0,084 & 0,105 & 0,023 & 0,048 \\ 0,012 & 0,084 & 0,023 & 0,105 & 0,048 \\ 0,012 & 0,031 & 0,105 & 0,105 & 0,073 \\ 0,012 & 0,031 & 0,105 & 0,023 & 0,073 \\ 0,012 & 0,084 & 0,023 & 0,105 & 0,048 \\ 0,012 & 0,084 & 0,023 & 0,023 & 0,073 \\ 0,129 & 0,031 & 0,023 & 0,105 & 0,073 \\ 0,012 & 0,031 & 0,105 & 0,023 & 0,073 \\ 0,129 & 0,084 & 0,023 & 0,023 & 0,073 \\ 0,012 & 0,031 & 0,023 & 0,023 & 0,073 \end{pmatrix}$$

Каждый столбец этой матрицы представляет собой «собственный» вектор матрицы парных сравнений критериев.

Здесь, например,

$$D_4(p_3) = \frac{w_4^3}{\sum_{j=1}^n w_j^3} = \frac{1}{e^{\frac{6}{4}} + e^{\frac{6}{4}} + e^{\frac{6}{4}} + 1 + e^{\frac{6}{4}} + e^{\frac{6}{4}} + 1 + e^{\frac{6}{4}} + e^{\frac{6}{4}} + 1 + 1 + 1 + e^{\frac{6}{4}} + 1 + 1} \approx 0,023.$$

$$D_3(p_4) = \frac{w_3^4}{\sum_{j=1}^n w_j^4} = \frac{e^{\frac{6}{4}}}{e^{\frac{6}{4}} + e^{\frac{6}{4}} + e^{\frac{6}{4}} + e^{\frac{6}{4}} + 1 + 1 + e^{\frac{6}{4}} + e^{\frac{6}{4}} + 1 + e^{\frac{6}{4}} + 1 + e^{\frac{6}{4}} + 1 + 1 + 1} \approx 0,105.$$

Теперь посчитаем оценку ущерба для каждой из 15 альтернатив-ролей.

$$D(r_1) = \sum_{k=1}^m P(p_k)D_1(p_k) \approx 0,14 \times 0,129 + 0,23 \times 0,084 + 0,16 \times 0,105 + 0,17 \times 0,105 + 0,3 \times 0,073 \approx 0,098,$$

$$D(r_2) = \sum_{k=1}^m P(p_k)D_2(p_k) \approx 0,14 \times 0,129 + 0,23 \times 0,084 + 0,16 \times 0,105 + 0,17 \times 0,105 + 0,3 \times 0,048 \approx 0,086,$$

$$D(r_3) = \sum_{k=1}^m P(p_k)D_3(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,084 + 0,16 \times 0,105 + 0,17 \times 0,105 + 0,3 \times 0,073 \approx 0,078,$$

$$D(r_4) = \sum_{k=1}^m P(p_k)D_4(p_k) \approx 0,14 \times 0,129 + 0,23 \times 0,084 + 0,16 \times 0,023 + 0,17 \times 0,105 + 0,3 \times 0,073 \approx 0,081,$$

$$D(r_5) = \sum_{k=1}^m P(p_k)D_5(p_k) \approx 0,14 \times 0,129 + 0,23 \times 0,084 + 0,16 \times 0,105 + 0,17 \times 0,023 + 0,3 \times 0,073 \approx 0,080,$$

$$D(r_6) = \sum_{k=1}^m P(p_k)D_6(p_k) \approx 0,14 \times 0,129 + 0,23 \times 0,084 + 0,16 \times 0,105 + 0,17 \times 0,023 + 0,3 \times 0,048 \approx 0,072,$$

$$D(r_7) = \sum_{k=1}^m P(p_k)D_7(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,084 + 0,16 \times 0,023 + 0,17 \times 0,105 + 0,3 \times 0,048 \approx 0,057,$$

$$D(r_8) = \sum_{k=1}^m P(p_k)D_8(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,031 + 0,16 \times 0,105 + 0,17 \times 0,105 + 0,3 \times 0,073 \approx 0,066,$$

$$D(r_9) = \sum_{k=1}^{m} P(p_k)D_9(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,031 + 0,16 \times 0,105 + 0,17 \times 0,023 + 0,3 \times 0,073 \approx 0,052,$$

$$D(r_{10}) = \sum_{k=1}^{m} P(p_k)D_{10}(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,084 + 0,16 \times 0,023 + 0,17 \times 0,105 + 0,3 \times 0,048 \approx 0,057,$$

$$D(r_{11}) = \sum_{k=1}^{m} P(p_k)D_{11}(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,084 + 0,16 \times 0,023 + 0,17 \times 0,023 + 0,3 \times 0,073 \approx 0,051,$$

$$D(r_{12}) = \sum_{k=1}^{m} P(p_k)D_{12}(p_k) \approx 0,14 \times 0,129 + 0,23 \times 0,031 + 0,16 \times 0,023 + 0,17 \times 0,105 + 0,3 \times 0,073 \approx 0,069,$$

$$D(r_{13}) = \sum_{k=1}^{m} P(p_k)D_{13}(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,031 + 0,16 \times 0,105 + 0,17 \times 0,023 + 0,3 \times 0,073 \approx 0,052,$$

$$D(r_{14}) = \sum_{k=1}^{m} P(p_k)D_{14}(p_k) \approx 0,14 \times 0,129 + 0,23 \times 0,084 + 0,16 \times 0,023 + 0,17 \times 0,023 + 0,3 \times 0,073 \approx 0,067,$$

$$D(r_{15}) = \sum_{k=1}^{m} P(p_k)D_{15}(p_k) \approx 0,14 \times 0,012 + 0,23 \times 0,031 + 0,16 \times 0,023 + 0,17 \times 0,023 + 0,3 \times 0,073 \approx 0,039.$$

Прокомментируем полученные результаты.

Во-первых, довольно ожидаемо, что чем больше полномочий приписано роли, тем больше ущерб в результате успешной атаки на нее. Это, однако, не всегда верно. Можно построить пример, в котором роль, которой приписано единственное «ценное» (редкое) полномочие, получит большую оценку, чем роль, которой приписано несколько распространенных полномочий, ущерб от утечки которых невелик.

Во-вторых, если сравнивать роли с одинаковым числом полномочий, то чем больше полномочий, утечка которых приводит к большому ущербу, приписано роли, тем выше оценка ущерба этой роли. В условиях, когда коэффициенты относительного ущерба $v_k$ определяются эвристически согласно предложенному правилу, данный факт можно интерпретировать следующим образом: чем больше приписано роли редко встречающихся полномочий, тем выше ее оценка ущерба. Так, например, в нашем примере среди всех ролей, которым приписано по три полномочия, наивысшую оценку получила роль $r_6$, которой не приписано самое распространенное полномочие $p_5$, зато приписано редкое полномочие $p_1$. Разница в оценках, однако, не велика, так как все полномочия представлены в графе ролей достаточно широко, к тому же $r_6$ содержит второе по популярности полномочие $p_2$.

По той же причине среди всех ролей, которым приписаны по два полномочия, по оценке лидируют $r_7$ и $r_{10}$.

В третьих, оценка относительного ущерба тем выше, чем выше вероятность утечки полномочия, приписанного роли. Это, однако, второстепенный фактор, поскольку высокая вероятность похищения определенного полномочия сама по себе еще не означает, что атака будет предпринята по отношению к конкретной роли, которой приписано данное полномочие. Но даже по нашему примеру можно заметить, что в лидерах по оценке относительного ущерба находятся роли с полномочием $p_2$. Как и $p_5$, это полномочие имеет высокую оценку риска утечки, но значительно реже встречается в листовых ролях (что повышает его «ценность» с точки зрения предложенных эвристик).

По результатам, полученным на выходе алгоритма, рекомендуется уделить повышенное внимание (в частности, в сфере повышения уровня защиты) тем (листовым) ролям, которые получили наиболее высокие оценки относительного ущерба. В первую очередь, это роли $r_6$ и $r_{12}$. При решении задачи авторизации [5] следует избегать назначения на эти роли пользователей при наличии альтернатив с меньшей оценкой.

## Список литературы


[1] D.F. Ferraiolo, D.R. Kuhn. Role-Based Access Control. *15th National Computer Security Conference*, 554–563, October 1992.

[2] D.N. Kolegov. Hierarchical Role-Based Access Control Development. *Prikladnaja diskretnaja matematika*, 3(17):70–76, 2012 (In Russian).

[3] T.L. Saaty. *The Analytic Hierarchy Process.* New York, McGraw Hill, 1980.

[4] S.V. Belim, N.F. Bogachenko. Using a Hierarchy Analysis Method to Assess Permission Leakage Risks in Systems with a Role Based Access Control. *Information and Control Systems*, 6(67):67–72, 2013 (in Russian).

[5] S.V. Belim, S.Yu. Belim, N.F. Bogachenko. Using Analytic Hierarchy Process for Building of Role Based Access Control. *Information Security Problems. Computer Systems*, 3:7–17, 2013 (in Russian).

## On the Estimation of the Damage from the Leakage of Permissions in a Role-Based Security Model

Sergey V. Usov, Nadezda F. Bogachenko

In this paper, we propose an algorithm for estimating the relative damage from leakage of permissions within the role-based access model with a hierarchy introduced on a set of roles. The relative damage is calculated using the analytic hierarchy process (AHP). A version of the relative damage estimation algorithm, which does not require involving of AHP's expert estimations, is provided.