Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, с. 45-48 (http://пниэи.рф/activity/science/BIT/T8-p45.pdf)

# УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ РАЗНОГО УРОВНЯ ДОВЕРИЯ

Беляев Д. Л., Нешин Д. В., Байбосын А. Б. (г. Орёл)

Приоритетное направление развития корпоративных мультисервисных сетей (МСС) связано с расширением перечня предоставляемых информационных и коммуникационных услуг. Для решения ряда задач пользователям требуется возможность доступа к ресурсам существующих корпоративных и открытых сетей с использованием одного универсального абонентского средства, позволяющего получить расширенный перечень инфокоммуникационных услуг. Применение всевозможных технических решений и организационных мер обеспечения информационной безопасности позволяет осуществить противодействие угрозам только со стороны внешнего нарушителя. Однако сохраняется возможность реализации внутренних угроз, в частности возможность утечки информации с защищаемых ресурсов.

Одним из возможных решений этой проблемы является контроль над процессами, выполняемыми в операционной системе и порождаемыми ими потоками. Управление доступом к информационным ресурсам разного уровня доверия предлагается осуществлять посредством запуска и остановки процессов в операционной системе, ассоциированных с подключением к ИР, и с применением локальных СЗИ, в зависимости от оценки защищённости автоматизированной системы (АС).

В процессе функционирования АС, одновременно подключённой к МСС разного уровня доверия, её защищённость обладает некоторой неопределённостью. В качестве исходных данных для оценивания защищённости АС могут быть использованы сведения, полученные при проведении экспертного опроса на основе метода теории нечётких множеств, заключающегося в применении парных сравнений на ранговых оценках [1, 2]. Шкала Саати для оценки вклада процессов в защищённость АС приведена в табл. 1.

Таблица 1 – Шкала относительной важности, используемая для построения матрицы суждений

| Лингвистическая переменная | Вклад процесса в защищённость АС ($\rho_{процесса}$) |
|---|---|
| Сильно повышает | 5 |
| Слабо повышает | 3 |
| Не влияет | 1 |
| Слабо уменьшает | ⅓ |
| Сильно уменьшает | ⅕ |
| Промежуточные значения | 4, 2, ½, ¼ |

Каждому процессу, разрешённому к выполнению в операционной системе, ставится в соответствие лингвистическая переменная, в зависимости от значения которой устанавливается вклад $n$-го процесса в защищённость АС ($\rho_n$). Относительные оценки рангов используются для построения матрицы парных

сравнений и вычисления функции принадлежности в соответствии с выражением (1), предложенным А. П. Ротштейном.

$$\left.\begin{aligned}
\mu_0 &= \left(1 + \frac{\rho_1}{\rho_0} + \frac{\rho_2}{\rho_0} + ... + \frac{\rho_N}{\rho_0}\right)^{-1} \\
\mu_1 &= \left(\frac{\rho_0}{\rho_1} + 1 + \frac{\rho_2}{\rho_1} + ... + \frac{\rho_N}{\rho_1}\right)^{-1} \\
&... \\
\mu_N &= \left(\frac{\rho_0}{\rho_N} + \frac{\rho_1}{\rho_N} + \frac{\rho_2}{\rho_N} + ... + 1\right)^{-1}
\end{aligned}\right\}, \qquad (1)$$

где $\rho_n$ – вклад *n*-го процесса в защищённость АС,

$\mu_n$ – степень принадлежности элементов нечёткого множества, характеризующего защищённость АС в случае выполнения n-го процесса.

Полученные значения после нормировки используются для расчёта защищённости АС при совместном выполнении *m* процессов в АС в соответствии с выражением (2).

$$\mu_m^{\Sigma} = \frac{\sum_{n=1}^{m} \overline{\mu}_n}{m}, \qquad (2)$$

где $\overline{\mu}_n$ – нормированное значение степени принадлежности защищённости АС при выполнении n-го процесса.

Результатом является ранжированное множество состояний защищённости, каждому из которых соответствует определённый перечень выполняемых процессов выражение (3).

$$X = \{(\min \mu_m^{\Sigma}) / x_1, ..., \mu_m^{\Sigma} / x_i, ..., (\max \mu_m^{\Sigma}) / x_I\}^T, \qquad (3)$$

Управление доступом к информационным ресурсам разного уровня доверия основывается на применении математического аппарата управляемых цепей Маркова [2]. Для определения вероятности перехода из *i*-го состояния в *j*-е подсчитывается частота переходов (рассчитывается доля случаев благоприятных,переходу в *j*-е состояние в общем их числе). Вычисленные вероятности переходов образуют квадратные матрицы $\left\| P_{ij}^{u_s}(k/k-1) \right\|$ размерности $I \times I$, каждая из которых соответствует запуску или остановке процессов в АС.

Оценка защищённости АС на *k*-м шаге для каждого управления рассчитывается из уравнения состояния конечномерной марковской последовательности, описываемой выражением (4).

$$x(k) = X^T \vec{\mu}(k), \qquad (4)$$

где $\vec{\mu}(k)$ – вектор, характеризующий состояние защищённости в k-й момент времени, рассчитываемый из уравнения Колмогорова-Чепмена:

$$\vec{\mu}(k) = \left\| P_{ij}^{u_s}(k/k-1) \right\|^T \vec{\mu}(k-1) = \begin{pmatrix} \mu_1^{u_s}(k) \\ \mu_2^{u_s}(k) \\ \dots \\ \mu_N^{u_s}(k) \end{pmatrix}. \quad (5)$$

Сравнение защищённостипо всем управлениям $u_s$ выполняется после скаляризации:

$$x^{u_s}(k) = \sum_{i=1}^{I} \left( \mu_i^{u_s}(k)\ x_i \right) \quad (6)$$

Сравнение прогнозных значений изменения состояний защищённости для разных управляющих воздействий позволяет выбрать те из них, в которых защищённость АС соответствует требуемому значению [3, 4]. Одинаковое состояние может быть достигнуто остановкой и запуском разного перечня процессов ОС. Рациональные стратегии выбора количества выполняемых процессов позволяют обеспечить более эффективное использование АС. При этом оптимизация реализуется в два этапа: вначале выполняется поиск состояний, в которых защищённость АС принимает наиболее высокое значение. На втором этапе выбирается управляющее воздействие, приводящее в данное состояние посредством ограничения минимального количества ИР и применением наименьшего количества СЗИ. Принимая количество процессов, которые необходимо остановить, в качестве потерь, может быть решена задача повышения своевременности доступа к информационным ресурсам МСС разного уровня доверия посредством методов динамического управления. Ожидаемые потери по всем состояниям защищённости АС в случае реализации управления $u_s$ представлены выражением 7.

$$\vec{r}(u_s) = \begin{pmatrix} r_0(u_s) \\ \dots \\ r_i(u_s) \\ \dots \\ r_I(u_s) \end{pmatrix}. \quad (7)$$

Априорное пошаговое значение количества останавливаемых процессов для *i*- го состояния на *k*-м шаге определяется прямым рекуррентным соотношением (функцией Беллмана) – выражением 8.

$$R_i\left(k, v = v_n, u_s(k)\right) = \min_{u_s} \left[ r_i\left(k, u_s(k)\right) + \sum_{j=1}^{I} p_{ij}^{u_s}(k/k-1) R_j\left(k-1, v = v_n, u_s(k-1)\right) \right], \quad (8)$$

где $R_j\left(k-1, v = v_n, u_s(k-1)\right)$ – потери для *j*-го состояния защищённости при условии выбора на *(k-1)*- м шаге адаптивного управления $u_s(k-1)$.

Анализ управлений, вычисленных согласно (8) для каждого из состояний защищённости, показал стационарность применяемых стратегий управления по шагам функционирования.

Данные выражения могут быть положены в основу алгоритма управления доступом к информационным ресурсам разного уровня доверия на основе оценки

защищённости автоматизированной системы. Реализация алгоритма должна способствовать обеспечению безопасности обрабатываемой информации при совместном доступе к информационным ресурсам разного уровня доверия и повышению своевременности предоставления информации в случае, если уровень доверия используемых информационных ресурсов одинаковый.

Литература

1. Иванов В.А. Прогнозирование состояния защищённости компьютерных систем на основе нечетких множеств, аппарата управляемых цепей Маркова и экспертно-рискового метода / В. А. Иванов, В. В. Комашинский, Д. Л. Беляев, И. В. Иванов // Телекоммуникации. – М.: «Наука и технологии», 2009. – №6. – С. 33-35.

2. Комашинский В.В. Методика управления информационной безопасностью вычислительной системы на основе оценки состояния защищённости / В. В. Комашинский, Д. Л. Беляев // Вестник компьютерных и информационных технологий. – М.: «Машиностроение», 2010. – №2 (68). С. 48-55.

3. Комашинский В. В., Беляев Д. Л. Описание к патенту на изобретение RU № 2436154. Способ управления доступом к информационным ресурсам компьютерных сетей различных уровней конфиденциальности и устройство, его реализующее; заявитель и патентообладатель Академия ФСО России. – Приоритет изобретения 1 декабря 2009 г. Зарегистрировано в Государственном реестре изобретений РФ 10 декабря 2011 г.

4. Беляев Д. Л., Комашинский В. В. Описание к патенту на полезную модель RU № 99880. Устройство управления доступом к информационным ресурсам мультисервисной сети; заявитель и патентообладатель Академия ФСО России. – Приоритет полезной модели 12 июля 2010 г. Зарегистрировано в Государственном реестре полезных моделей РФ 27 ноября 2010 г.

Материалы поступили 25.03.2012, опубликовано в Интернет 12.05.2012 по положительной рецензии д.т.н., доцента Иванова А.И. (Пенза).