С. В. Запечников

БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ ПРИ РАЗЛИЧНЫХ СТРАТЕГИЯХ РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ[1]

Введение

Устойчивость работы распределенных компьютерных систем (РКС) при разрушении, охватывающем всю или значительную часть системы, достигается за счет резервирования информационных ресурсов (ИР), основанного на введении информационной избыточности. Оно сводится к созданию идентичных копий ИР системы (или части системы) либо неидентичных копий — предысторий. Альтернативные подходы заключаются во введении в систему структурной либо временной избыточности. Наиболее глубокое исследование стратегий резервирования с точки зрения эффективности их функционирования в АСУ представлено в монографии [1]. В настоящей работе проводится исследование самых распространенных стратегий резервирования ИР в части их влияния на основные аспекты информационной безопасности ИР, а именно: доступность, целостность и конфиденциальность. Введем необходимые обозначения.

Пусть R — совокупность ИР системы в некоторый выделенный момент времени τ; $\overline{T}_{д}$, $\overline{T}_{ц}$, $\overline{T}_{к}$ — среднее время, которое требуется нарушителю для нарушения соответственно доступности, целостности либо конфиденциальности одной копии ИР; $\rho_{д} = \rho_{д}(r, \overline{T}_{д})$, $\rho_{ц} = \rho_{ц}(r, \overline{T}_{ц})$, $\rho_{к} = \rho_{к}(r, \overline{T}_{к})$, $0 < \rho_{д} < 1$, $0 < \rho_{ц} < 1$, $0 < \rho_{к} < 1$ — вероятности успеха нарушителя в нарушении доступности, целостности либо конфиденциальности одной копии за этот период времени; $q_{д} = 1 - \rho_{д}$, $q_{ц} = 1 - \rho_{ц}$, $q_{к} = 1 - \rho_{к}$ — вероятности отражения соответствующей атаки нарушителя; $\rho_{д}(R)$, $\rho_{ц}(R)$, $\rho_{к}(R)$ — вероятности успеха нарушителя в нарушении доступности, целостности либо конфиденциальности зарезервированных ИР; $\overline{T}_{д}^{(n)}$, $\overline{T}_{ц}^{(n)}$, $\overline{T}_{к}^{(n)}$ — среднее время, которое требуется нарушителю для нарушения доступности, целостности либо конфиденциальности n-кратно зарезервированных ИР. Если нарушитель добился успеха при атаке на одну из копий (предысторий) ИР, он начинает атаковать следующую.

1. Создание n копий информационных ресурсов

Основная копия $r^{(1)}$ резервируется копиями $r^{(2)},\ldots,r^{(n)}$. Обозначим: $n = s$.

Нарушение доступности. Граф состояний ИР при попытке нарушения доступности изображен на рис. 1.

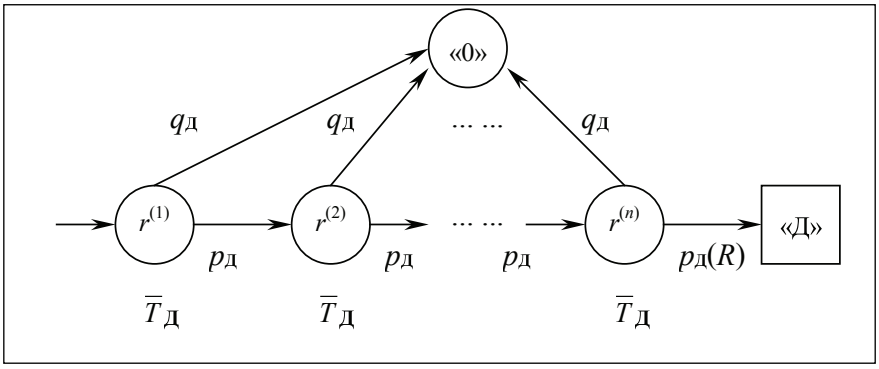


Рис. 1. Граф состояний ИР, зарезервированных n копиями, при попытке нарушения доступности

[1] Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 г.

Обозначения: $r^{(i)}$ — состояние ИР, характеризующееся утратой доступности i копий; «Д» — состояние ИР, характеризующееся полной утратой его доступности; «0» — состояние ИР, характеризующееся его доступностью и неудачей нарушителя в попытке нарушения доступности ИР.

Вероятностный процесс действий нарушителя описывается уравнением:

$$q_{Д} + q_{Д}p_{Д} + q_{Д}p_{Д}^{2} + \ldots + q_{Д}p_{Д}^{n-1} + q_{Д}p_{Д}^{n} = 1,$$
$$p_{Д}(R) = p_{Д}^{n}.$$

Кратность n резервирования, позволяющая добиться заданной величины $\rho_{Д}(R)$, определяется по формуле:

$$\hat{n}_{Д} = \left\lceil \frac{\ln p_{Д}(R)}{\ln p_{Д}} \right\rceil.$$

Среднее время, которое нарушитель затратит на нарушение доступности n копий, вне зависимости от того, сможет он блокировать все n копий или нет, составит:

$$\overline{T}_{Д}^{(n)} = \sum_{i=0}^{n-1} \overline{T}_{Д} \cdot (i+1) \cdot q_{Д} \cdot p_{Д}^{i} + \overline{T}_{Д} \cdot np_{Д}^{n} = \overline{T}_{1} + \overline{T}_{2},$$

где

$$\overline{T}_{1} = \overline{T}_{Д} \cdot \frac{q_{Д} \cdot \left(1 - 2p_{Д}^{1+(n-1)} - (n-1)p_{Д}^{1+(n-1)} + p_{Д}^{2+(n-1)} + (n-1)p_{Д}^{2+(n-1)}\right)}{(p_{Д} - 1)^{2}} =$$
$$\overline{T}_{Д} \cdot \frac{1 - p_{Д}^{n} \cdot (1 + nq_{Д})}{q_{Д}},$$
$$\overline{T}_{2} = \overline{T}_{Д} \cdot np_{Д}^{n};$$

откуда $\overline{T}_{Д}^{(n)} = \overline{T}_{Д} \cdot \frac{1 - p_{Д}^{n}(1 + nq_{Д}) + np_{Д}^{n}q_{Д}}{q_{Д}} = \overline{T}_{Д} \cdot \frac{1 - p_{Д}^{n}}{q_{Д}}.$

Нарушение целостности. Состояние ИР, при котором наступает нарушение их целостности, зависит от применяемого метода контроля. Будем рассматривать наихудший для защиты (и наилучший для нарушителя) случай. При мажоритарном контроле неверное значение r будет принято в качестве верного при модификации $\lceil n/2 \rceil$ копий.

Вывод конечных выражений для $\rho_{Ц}(R)$, $\hat{n}_{Ц}$ и $\overline{T}_{Ц}$ аналогичен предыдущему:

$$p_{Ц}(R) = p_{Ц}^{\lceil n/2 \rceil},\ \hat{n}_{Ц} = \left\lceil \frac{\ln p_{Ц}(R)}{\ln p_{Ц}} \right\rceil,\ \overline{T}_{Ц}^{(n)} = \overline{T}_{Ц} \cdot \frac{1 - p_{Ц}^{\lceil n/2 \rceil}}{q_{Ц}}.$$

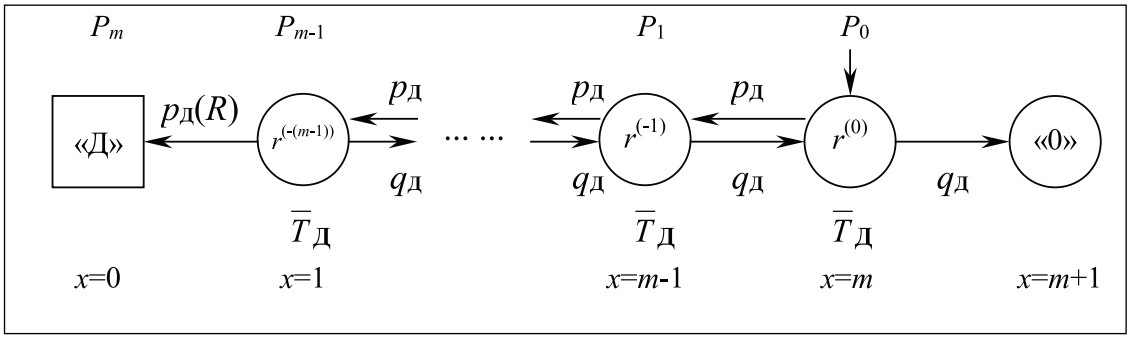
Нарушение конфиденциальности. Нарушение конфиденциальности ИР происходит при нарушении конфиденциальности хотя бы одной идентичной копии. Если нарушитель может компрометировать копии ИР вне зависимости от того, доступны эти копии в РКС или нет, то $p_{К}(R) = 1 - q_{К}^{n},\ \hat{n}_{К} = \left\lceil \frac{\ln(1 - p_{К}(R))}{\ln q_{К}} \right\rceil,\ \overline{T}_{К}^{(n)} = \overline{T}_{К}.$

Если нарушитель не может нарушить конфиденциальность недоступной в РКС копии ИР, то $p_{К}(R) = 1 - (1 - p_{К}q_{Д})^{n},\ \hat{n}_{К} = \left\lceil \frac{\ln(1 - p_{К}(R))}{\ln(1 - p_{К}q_{Д})} \right\rceil,\ \overline{T}_{К}^{(n)} = \overline{T}_{К} \cdot \frac{1 - p_{К}q_{Д}}{q_{К}}.$

2. Создание m предысторий информационных ресурсов

Основная копия $r^{(0)}$ резервируется предысториями $\{r^{(-1)}, ..., r^{(-(m-1))}\}$. Обозначим: m = s.

Нарушение доступности. Граф состояний информационных ресурсов при попытке нарушения доступности ресурсов изображен на рис. 2.



Обозначения: $r^{(-j)}$ — состояние ИР, характеризующееся утратой доступности всех предысторий с номерами от 0 до j включительно; «Д» — состояние ИР, характеризующееся полной утратой его доступности; «0» — состояние ИР, характеризующееся его доступностью и неудачей нарушителя в попытке нарушения доступности ИР.

Рис. 2. Граф состояний ИР, зарезервированных m предысториями, при попытке нарушения доступности

Вероятностный процесс действий нарушителя при этом описывается классической «задачей о разорении» [2. С. 109–120]. Утрата доступности произойдет при разрушении всех m предысторий.

Будем интерпретировать исходы воздействия нарушителя на каждую из предысторий как перемещения точки вправо-влево по вершинам графа. В начальный момент она находится в вершине $r^{(0)}$, а через периоды времени $\overline{T}_д$ перемещается на один шаг влево или вправо в зависимости от успеха или неудачи соответствующего воздействия нарушителя. Пронумеруем вершины графа от крайней левой $x = 0$ до крайней правой $x = m + 1$ и обозначим P_x — вероятность разорения при условии нахождения в начальный момент времени в вершине с номером x. Положение точки в каждый момент времени определяет количество неразрушенных предысторий. Если ИР находятся в состоянии x, то после каждого воздействия нарушителя они переходят в состояние $x \pm 1$. Атака нарушителя успешна, если точка попадет в крайнюю левую вершину. Обозначим вероятность этого события через $\rho_д(R)$. Поскольку в начальный момент точка находится в вершине с номером $x = m$, то $\rho_д(R) = P_m$. Запишем уравнение траектории блужданий частицы в «задаче о разорении» при $1 < x < m + 1$:

$$P_x = P_{x+1} q_д + P_{x-1} p_д . \quad (1)$$

Начальные условия для уравнения задаются следующим образом: $P_0 = 1$, $P_{m+1} = 0$.

Можно показать, что решение уравнения (1) записывается в виде:

$$p_д(R) = \begin{cases} \dfrac{p_д^m \cdot |p_д - q_д|}{|p_д^{m+1} - q_д^{m+1}|}, \text{ если } p_д \neq q_д, \\ \dfrac{1}{m+1}, \text{ если } p_д = q_д . \end{cases} \quad (2)$$

Из формулы (2) следует оценка числа предысторий $\hat{m}_д$ для достижения заданной вероятности $\rho_д(R)$:

$$\hat{m}_{\text{Д}} = \begin{cases} \left\lceil \ln\left(1-\dfrac{1-q_{\text{Д}}/p_{\text{Д}}}{1-p_{\text{Д}}(R)}\right) \Big/ \ln\left(q_{\text{Д}}/p_{\text{Д}}\right) \right\rceil - 1, \text{ если } p_{\text{Д}} \neq q_{\text{Д}}, \\ \left\lceil \dfrac{1}{p_{\text{Д}}(R)} \right\rceil - 1, \text{ если } p_{\text{Д}} = q_{\text{Д}}. \end{cases}$$

Если t_x — средняя продолжительность периода времени от начала атаки нарушителя до утраты доступности всех копий ИР либо до окончания атаки, то средняя продолжительность атаки нарушителя вне зависимости от того, добьется он успеха или нет, определяется путем решения разностного уравнения:

$$t_x = q_{\text{Д}} t_{x+1} + p_{\text{Д}} t_{x-1} + 1$$

при $1 < x < m+1$, с начальными условиями: $t_0 = 0$, $t_{m+1} = 0$,

откуда

$$\overline{T}_{\text{Д}}^{(m)} = \overline{T}_{\text{Д}} \cdot t_{k+1} \; \frac{\overline{T}_{\text{Д}}}{p_{\text{Д}} - q_{\text{Д}}} \cdot \left(m - (m+1) \cdot \frac{1-\left(p_{\text{Д}}/q_{\text{Д}}\right)^m}{1-\left(p_{\text{Д}}/q_{\text{Д}}\right)^{m+1}} \right), \text{ если } p_{\text{Д}} \neq q_{\text{Д}},$$

$$m \cdot \overline{T}_{\text{Д}}, \text{ если } p_{\text{Д}} = q_{\text{Д}}.$$

Нарушение целостности. В этом случае достаточно (в худшей с точки зрения защиты ситуации) нарушить целостность хотя бы одной предыстории в то время, когда она используется в штатном режиме либо для получения других предысторий. Поэтому с учетом ранее полученных результатов по доступности будем иметь:

$$p_{\text{Ц}}(R) = 1 - \prod_{i=0}^{m-1} \left(1 - p_{\text{Ц}} \cdot P_{\text{Д}}^{(i)}\right),$$

где $\rho_{\text{Д}}^{(i)}$ — вероятность того, что предыстория $r^{(-i)}$ является рабочей копией. Отсюда

$$p_{\text{Ц}}(R) = 1 - \prod_{i=0}^{m-1} \left(1 - p_{\text{Ц}} \cdot p_{\text{Д}}^{i}\right).$$

Оценку числа предысторий $\hat{m}_{\text{Ц}}$ для достижения заданной вероятности $\rho_{\text{Ц}}(R)$ следует находить численными методами.

Средняя продолжительность атаки нарушителя вне зависимости от того, добьется он успеха или нет:

$$\overline{T}_{\text{Ц}}^{(m)} = \overline{T}_{\text{Ц}} p_{\text{Ц}} \cdot \sum_{i=0}^{m-1} p_{\text{Д}}^{i}.$$

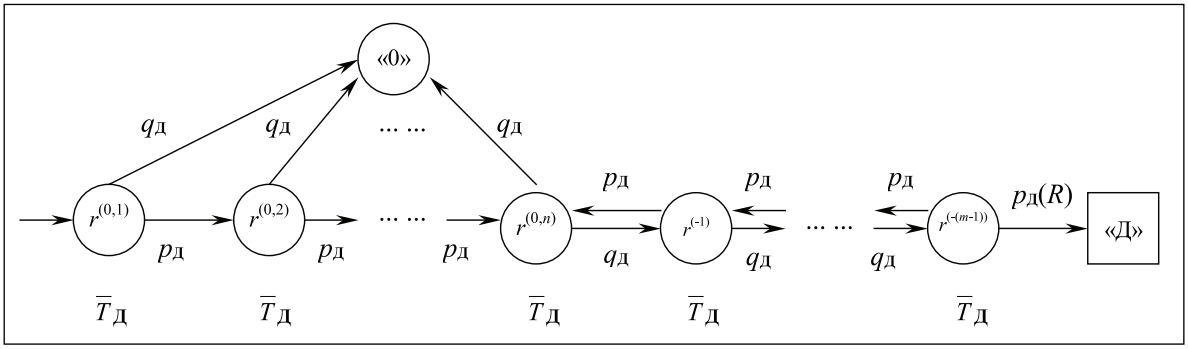
Нарушение конфиденциальности ИР для рассматриваемой стратегии происходит при нарушении конфиденциальности хотя бы одной копии (в данном случае неидентичной). Если нарушитель может компрометировать копии ИР вне зависимости от того, доступны эти копии в РКС или нет, то $p_{\text{К}}(R) = 1 - q_{\text{К}}^{m}$, $\hat{m}_{\text{К}} = \left\lceil \dfrac{\ln(1-p_{\text{К}}(R))}{\ln q_{\text{К}}} \right\rceil$, $\overline{T}_{\text{К}}^{(m)} = \overline{T}_{\text{К}}$.

Если нарушитель не может скомпрометировать недоступные в РКС копии ИР, то тогда $p_{\text{К}}(R) = 1 - \left(1 - p_{\text{К}} q_{\text{Д}}\right)^m$, $\hat{m}_{\text{К}} = \left\lceil \dfrac{\ln(1-p_{\text{К}}(R))}{\ln\left(1-p_{\text{К}} q_{\text{Д}}\right)} \right\rceil$, $\overline{T}_{\text{К}}^{(m)} = \overline{T}_{\text{К}} \cdot \dfrac{1-p_{\text{К}} q_{\text{Д}}}{q_{\text{К}}}$.

3. Комбинированная стратегия: создание n копий и m предысторий ИР

Основная копия $r^{(0,1)}$ резервируется копиями $\{r^{(0,2)}, \ldots, r^{(0,\,n)}\}$ и предысториями $\{r^{(-1)}, \ldots, r^{(-(m-1))}\}$. Обозначим: $n + m = s$. При исследовании показателей безопасности для этого случая можно воспользоваться результатами, полученными для двух предыдущих стратегий.

Нарушение доступности. Граф состояний информационных ресурсов при попытке нарушения доступности ресурсов изображен на рис. 3.



Обозначения: $r^{(i)}$ — состояние ИР, характеризующееся утратой доступности i копий; $r^{(-j)}$ — состояние ИР, характеризующееся утратой доступности всех предысторий с номерами от 0 до j включительно; «Д» — состояние ИР, характеризующееся полной утратой его доступности; «0» — состояние ИР, характеризующееся его доступностью и неудачей нарушителя в попытке нарушения доступности ИР.

Рис. 3. Граф состояний ИР, зарезервированных n копиями и m предысториями, при попытке нарушения доступности

Принимая во внимание ранее полученные результаты, имеем:

$$p_д(R)= p_д^n \cdot p_д\left(r^{(-(m-1))}\right)=\begin{cases} p_д^n \cdot \dfrac{p_д^m \cdot \left|p_д - q_д\right|}{\left|p_д^{m+1} - q_д^{m+1}\right|} = \dfrac{p_д^s \cdot \left|p_д - q_д\right|}{\left|p_д^{m+1} - q_д^{m+1}\right|}, \\ \text{если } p_д \neq q_д, \\ \dfrac{p_д^n}{m+1} = \dfrac{1}{2^n \cdot (m+1)}, \text{ если } p_д = q_д. \end{cases} \quad (3)$$

Из формулы (3) следует оценка числа предысторий $\hat{m}_д$ для достижения заданной вероятности $\rho_д(R)$ при заданном числе копий:

$$\hat{m}_д = \begin{cases} \left\lceil \ln\left(1 - \dfrac{\left(1 - q_д/p_д\right)p_д^n}{p_д(R)}\right) \Big/ \ln\dfrac{q_д}{p_д} \right\rceil - 1, \text{ если } p_д \neq q_д, \\ \left\lceil \dfrac{p_д(R)}{p_д^n} \right\rceil - 1 = \left\lceil 2^n \cdot p_д(R) \right\rceil - 1, \text{ если } p_д = q_д, \end{cases}$$

а также оценка числа копий $\hat{n}_д$ для достижения заданной вероятности $\rho_д(R)$ при заданном числе предысторий:

$$\hat{n}_д = \begin{cases} \left\lceil \ln\left(\dfrac{p_д(R) \cdot \left|p_д^{m+1} - q_д^{m+1}\right|}{p_д^m \cdot \left|p_д - q_д\right|}\right) \Big/ \ln p_д \right\rceil, \text{ если } p_д \neq q_д, \\ \left\lceil \dfrac{\ln\left((m+1) \cdot p_д(R)\right)}{\ln(1/2)} \right\rceil, \text{ если } p_д = q_д. \end{cases}$$

Средняя продолжительность атаки нарушителя вне зависимости от того, добьется ли он успеха, определяется из уравнения:

$$\left(\frac{1-p_{\text{Д}}^{n}}{q_{\text{Д}}}+\frac{1}{\left|p_{\text{Д}}-q_{\text{Д}}\right|}\cdot\left|m-(m+1)\cdot\frac{\left|1-(p_{\text{Д}}/q_{\text{Д}})^{m}\right|}{\left|1-(p_{\text{Д}}/q_{\text{Д}})^{m+1}\right|}\right|-1\right)\cdot\overline{T}$$

$\overline{T}_{\text{Д}}^{(s)}=\overline{T}_{\text{Д}}^{(n)}+\overline{T}_{\text{Д}}^{(m)}$, если $p_{\text{Д}}\neq q_{\text{Д}}$,

$$\left(\frac{1-p_{\text{Д}}^{n}}{q_{\text{Д}}}+m\right)\cdot\overline{T}_{\text{Д}}=\left(2+m-2^{-n+1}\right)\overline{T}_{\text{Д}},\ \text{если}\ p_{\text{Д}}=q_{\text{Д}}.$$

Нарушение целостности. Результаты непосредственно следуют из результатов, полученных для 1-й и 2-й стратегий резервирования:

$$p_{\text{Ц}}(R)=\begin{cases}1-\left(1-p_{\text{Ц}}^{\lceil n/2\rceil}\right)\prod_{i=1}^{m-1}\left(1-\dfrac{p_{\text{Д}}^{n+i}p_{\text{Ц}}\cdot\left|p_{\text{Д}}-q_{\text{Д}}\right|}{\left|p_{\text{Д}}^{i+1}-q_{\text{Д}}^{i+1}\right|}\right), & \\ \text{если}\ p_{\text{Д}}\neq q_{\text{Д}}, & \\ 1-\left(1-p_{\text{Ц}}^{\lceil n/2\rceil}\right)\prod_{i=1}^{m-1}\left(1-\dfrac{p_{\text{Д}}^{n}p_{\text{Ц}}}{i+1}\right), & \text{если}\\ p_{\text{Д}}=q_{\text{Д}}, & \end{cases} \tag{4}$$

$$\overline{T}_{\text{Ц}}^{(s)}=\begin{cases}\left(\dfrac{1-p_{\text{Ц}}^{\lceil n/2\rceil}}{q_{\text{Ц}}}+\left|p_{\text{Д}}-q_{\text{Д}}\right|\cdot p_{\text{Ц}}\cdot\sum_{i=1}^{m-1}\dfrac{p_{\text{Д}}^{n+i}}{\left|p_{\text{Д}}^{i+1}-p_{\text{Д}}^{i+1}\right|}\right)\cdot\overline{T}_{\text{Ц}}, \text{если} & \\ p_{\text{Д}}\neq q_{\text{Д}}, & \\ \left(\dfrac{1-p_{\text{Ц}}^{\lceil n/2\rceil}}{q_{\text{Ц}}}+p_{\text{Д}}^{n}p_{\text{Ц}}\cdot\sum_{i=1}^{m-1}\dfrac{1}{i+1}\right)\cdot\overline{T}_{\text{Ц}}, \text{если}\ p_{\text{Д}}=q_{\text{Д}}. & \end{cases}$$

Нарушение конфиденциальности ИР для рассматриваемой стратегии, как и ранее, происходит при нарушении конфиденциальности хотя бы одной его копии (в данном случае неидентичной). Если нарушитель может компрометировать копии ресурсов вне зависимости от того, доступны или нет эти копии в РКС, то

$$p_{\text{К}}(R)=1-q_{\text{К}}^{s},\ \hat{n}_{\text{К}}=\left\lceil\frac{\ln(1-p_{\text{К}}(R))}{\ln q_{\text{К}}}\right\rceil-m,\ \hat{m}_{\text{К}}=\left\lceil\frac{\ln(1-p_{\text{К}}(R))}{\ln q_{\text{К}}}\right\rceil-n,\ \overline{T}_{\text{К}}^{(s)}=\overline{T}_{\text{К}}.$$

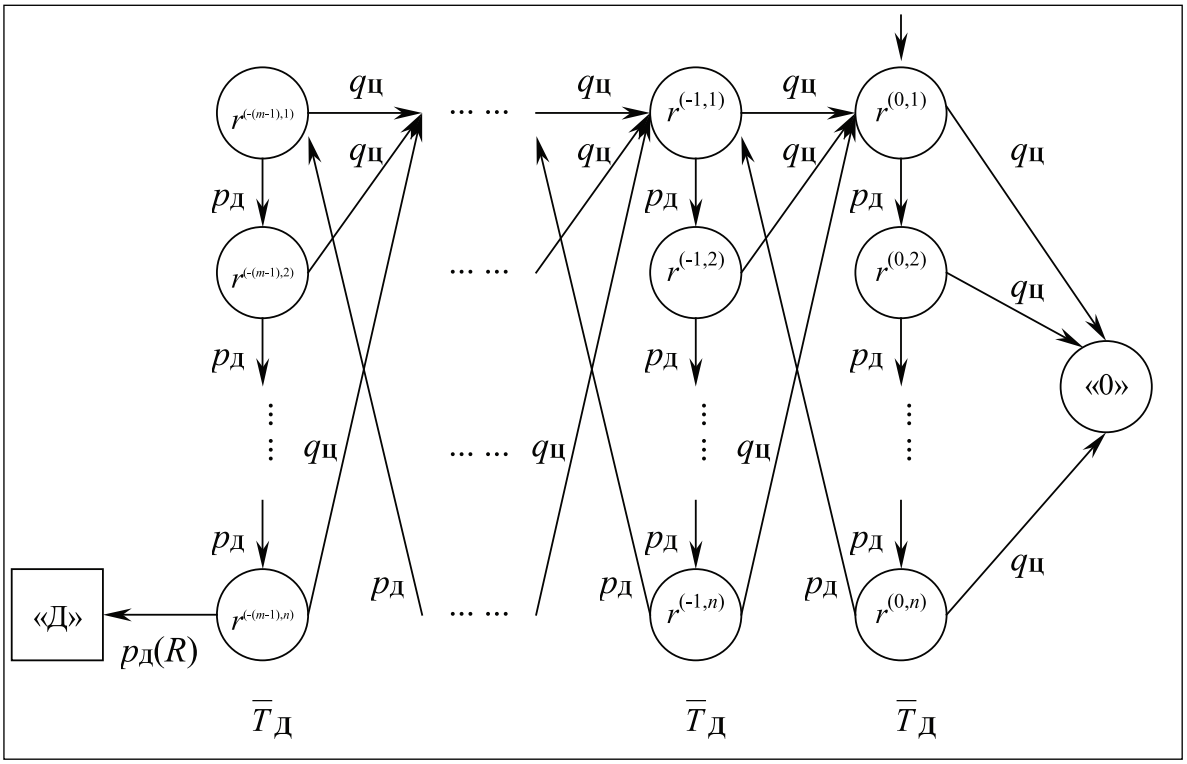
Если же компрометация нарушителем недоступных в РКС копий ИР невозможна, то тогда $p_{\text{К}}(R)=1-\left(1-p_{\text{К}}\left(1-p_{\text{Д}}\right)\right)^{s}$, $\hat{n}_{\text{К}}=\left\lceil\dfrac{\ln(1-p_{\text{К}}(R))}{\ln(1-p_{\text{К}}q_{\text{Д}})}\right\rceil-m$, $\hat{m}_{\text{К}}=\left\lceil\dfrac{\ln(1-p_{\text{К}}(R))}{\ln(1-p_{\text{К}}q_{\text{Д}})}\right\rceil-n$, $\overline{T}_{\text{К}}^{(m)}=\overline{T}_{\text{К}}\cdot\dfrac{1-p_{\text{К}}q_{\text{Д}}}{q_{\text{К}}}$.

4. Комбинированная стратегия: создание n копий каждой из m предысторий ИР

Основная копия $r^{(0,1)}$ резервируется копиями $\{r^{(0,2)}, \ldots, r^{(0,n)}\}$, а также предысториями $\{r^{(-1)}, \ldots, r^{(-(m-1))}\}$, каждая из которых представлена в n копиях: $\{\{r^{(-1,1)}, \ldots, r^{(-1,n)}\}, \ldots, \{r^{(-(m-1),1)}, \ldots, r^{(-(m-1),n)}\}$. Обозначим $nm = s$.

Нарушение доступности. Граф состояний ИР для рассматриваемой стратегии резервирования изображен на рис. 4. От построенного графа состояний ИР можно перейти к

укрупненному графу, стянув все вершины каждого из столбцов в одну вершину. Тогда задача сводится к рассмотренному ранее случаю, представляющему собой классическую «задачу о разорении», но с вероятностями переходов между состояниями, получаемыми из вероятностей $\rho_д$ и $q_д$ по следующим формулам: $\rho'_д = \rho^n_д$, $q'_д = 1-\rho^n_д$, и средним временем до разрушения всех копий одной предыстории, определяемым по формуле: $\overline{T}'_д = \frac{q'_д}{q_д} \cdot \overline{T}_д = \frac{1-p^n_д}{q_д} \cdot \overline{T}_д$.



Обозначения: r(i,-j) — состояние ИР, характеризующееся утратой доступности всех копий предысторий с номерами от 0 до j — 1 включительно и i копий j-й предыстории; «Д» — состояние ИР, характеризующееся полной утратой его доступности; «0» — состояние ИР, характеризующееся его доступностью и неудачей нарушителя в попытке нарушения доступности ИР.

Рис. 4. Граф состояний ИР, зарезервированных n копиями каждой из m предысторий, при попытке нарушения доступности

Отсюда

$$p_д(R): \begin{cases} \dfrac{(p'_д)^m \cdot |p'_д - q'_д|}{|(p'_д)^{m+1} - (q'_д)^{m+1}|} = \dfrac{p^{nm}_д \cdot |2p^n_д - 1|}{|p^{n(m+1)}_д - (1-p^n_д)^{m+1}|}, \text{ если } p_д \neq q_д, \\ \dfrac{1}{m+1}, \text{ если } p_д = q_д. \end{cases} \quad (5)$$

Число предысторий $\hat{m}_д$ при заданном числе копий и число копий $\hat{n}_д$ при заданном числе предысторий для достижения заданной вероятности $\rho_д(R)$ аналитически не выражаются, поэтому их следует находить численными методами.

Среднее время, затрачиваемое нарушителем на атаку:

$$\overline{T}_{\text{Д}}^{(s)} = \overline{T}_{\text{Д}} \cdot \left[\frac{1-p_{\text{Д}}^{n+1}}{q_{\text{Д}}} \left[\frac{1}{2p_{\text{Д}}^{n+1}-1} \left(m-(m+1)\cdot \frac{1-\left(\frac{p_{\text{Д}}^{n+1}}{1-p_{\text{Д}}^{n+1}}\right)^{m}}{1-\left(\frac{p_{\text{Д}}^{n+1}}{1-p_{\text{Д}}^{n+1}}\right)^{m+1}} \right) -1 \right] +1 \right], \text{ если } p_{\text{Д}} \neq q_{\text{Д}},$$

$$\overline{T}_{\text{Д}}^{(s)} = m\overline{T}'_{\text{Д}} + \overline{T}_{\text{Д}} = \overline{T}_{\text{Д}} \cdot \left(\frac{1-p_{\text{Д}}^{n}}{q_{\text{Д}}} \cdot m + 1 \right) = \overline{T}_{\text{Д}} \cdot \left(2m \cdot \left(1-2^{-n} \right) + 1 \right), \text{ если } p_{\text{Д}} = q_{\text{Д}}.$$

Нарушение целостности. Как и для 1-й стратегии, вероятность нарушения целостности каждой предыстории зависит от применяемого метода контроля. При мажоритарном контроле, принимая во внимание ранее полученные результаты, имеем:

$$p_{\text{Ц}}(R) = 1 - \prod_{i=0}^{m-1} \left(1 - p'_{\text{Ц}} \left(P'_{\text{Д}} \right)^{(i)} \right),$$

где $\rho'_{\text{Ц}}$ — вероятность нарушения целостности одной предыстории, зарезервированной n идентичными копиями, $(\rho'_{\text{Д}})^{(i)}$ — вероятность того, что рабочей копией является одна из копий предысторий $(r^{-i,k})$, где $k = \overline{1,n}$.

Таким образом,

$$p_{\text{Ц}}(R) = \begin{cases} 1 - \prod_{i=0}^{m-1} \left(1 - \dfrac{p_{\text{Д}}^{ni} p_{\text{Ц}}^{\lceil n/2 \rceil} \cdot \left| p_{\text{Д}} - q_{\text{Д}} \right|}{\left| p_{\text{Д}}^{n(i+1)} - \left(1-p_{\text{Д}}^{n} \right)^{i+1} \right|} \right), \text{ если } p_{\text{Д}} \neq q_{\text{Д}}, \\ 1 - \prod_{i=0}^{m-1} \left(1 - \dfrac{p_{\text{Ц}}^{\lceil n/2 \rceil}}{i+1} \right), \text{ если } p_{\text{Д}} = q_{\text{Д}}. \end{cases} \quad (6)$$

Число предысторий $\hat{m}_{\text{Ц}}$ при заданном числе копий и число копий $\hat{m}_{\text{Ц}}$ при заданном числе предысторий для достижения заданной вероятности $\rho_{\text{Ц}}(R)$ также в данном случае аналитически не выражаются.

Среднее время, затрачиваемое нарушителем на атаку:

$$\overline{T}_{\text{Ц}}^{(s)} = \overline{T}'_{\text{Ц}} \cdot \sum_{i=0}^{m-1} p'_{\text{Ц}} \left(P'_{\text{Д}} \right)^{(i)},$$

где $\overline{T}'_{\text{Ц}}$ — среднее время нарушения целостности одной предыстории, зарезервированной n идентичными копиями.

Таким образом,

$$\overline{T}_{\text{Ц}}^{(s)} = \begin{cases} \overline{T}_{\text{Ц}} \cdot \dfrac{\left| p_{\text{Д}} - q_{\text{Д}} \right| \cdot \left(1 - p_{\text{Ц}}^{\lceil n/2 \rceil} \right)}{q_{\text{Ц}}} \cdot \sum_{i=0}^{m-1} \dfrac{p_{\text{Д}}^{n+i}}{\left| p_{\text{Д}}^{i+1} - q_{\text{Д}}^{i+1} \right|}, \text{ если } p_{\text{Д}} \neq q_{\text{Д}}, \\ \overline{T}_{\text{Ц}} \cdot \dfrac{p_{\text{Д}}^{n} \cdot \left(1 - p_{\text{Ц}}^{\lceil n/2 \rceil} \right)}{q_{\text{Ц}}} \cdot \sum_{i=0}^{m-1} \dfrac{1}{i+1}, \text{ если } p_{\text{Д}} = q_{\text{Д}}. \end{cases}$$

Нарушение конфиденциальности ИР для рассматриваемой стратегии, как и ранее, происходит при нарушении конфиденциальности хотя бы одной его идентичной либо неидентичной копии. Если нарушитель может компрометировать копии ресурсов вне зависимости от того, доступны или нет эти копии в РКС, то

$$p_{\text{К}}(R) = 1 - q_{\text{К}}^{s}, \ \hat{n}_{\text{К}} = \left\lceil \frac{1}{m} \cdot \frac{\ln\left(1 - p_{\text{К}}(R)\right)}{\ln q_{\text{К}}} \right\rceil, \ \hat{m}_{\text{К}} = \left\lceil \frac{1}{n} \cdot \frac{\ln\left(1 - p_{\text{К}}(R)\right)}{\ln q_{\text{К}}} \right\rceil, \ \overline{T}_{\text{К}}^{(s)} = \overline{T}_{\text{К}}.$$

Если компрометация нарушителем недоступных в РКС копий ИР невозможна, то

$$p_{\text{К}}(R)=1-\left(1-p_{\text{К}}q_{\text{Д}}\right)^{s},\ \hat{n}_{\text{К}}=\left\lceil\frac{1}{m}\cdot\frac{\ln\left(1-p_{\text{К}}(R)\right)}{\ln\left(1-p_{\text{К}}q_{\text{Д}}\right)}\right\rceil,\ \hat{m}_{\text{К}}=\left\lceil\frac{1}{n}\cdot\frac{\ln\left(1-p_{\text{К}}(R)\right)}{\ln\left(1-p_{\text{К}}q_{\text{Д}}\right)}\right\rceil,\ \overline{T}_{\text{К}}^{(m)}=\overline{T}_{\text{К}}\cdot\frac{1-p_{\text{К}}q_{\text{Д}}}{q_{\text{К}}}.$$

5. Сравнительный анализ исследованных стратегий резервирования

В качестве единого критерия сравнения показателей доступности различных стратегий выберем $\alpha = \rho_{\text{Д}}(R)\big|_s$, в качестве критерия сравнения показателей целостности — $\beta = \rho_{\text{Ц}}(R)\big|_s$, в качестве критерия сравнения показателей конфиденциальности — $\gamma = \rho_{\text{К}}(R)\big|_s$, где s было определено ранее для каждой стратегии.

Из проведенного сравнения стратегий резервирования следуют *выводы*:

- ни одна из стратегий резервирования не позволяет повысить показатели конфиденциальности ИР;
- показатели доступности и целостности изменяются сложным образом, поэтому требуют дополнительного сопоставления.

Тем не менее отметим очевидное достоинство предложенного подхода. Оно заключается в том, что вероятности нарушения доступности, целостности и конфиденциальности могут быть определены одним из известных методов:

- пользуясь многорубежной моделью защиты и характеризуя $\overline{\text{Т}}_{\text{Д}}$, $\overline{\text{Т}}_{\text{Ц}}$, $\overline{\text{Т}}_{\text{К}}$ как среднее время преодоления одной из преград либо некоторого множества преград;
- пользуясь понятиями угроз и уязвимостей, находить $\rho_{\text{Д}}$, $\rho_{\text{Ц}}$, $\rho_{\text{К}}$ из выражений $p_{\mathbf{X}}=1-\left(1-\prod_{(i,j)\in I\times J}p_{T_i}\left(\overline{T}_{\mathbf{X}}\right)\cdot p_{V_j}\right)$, где $I\times J$ — номенклатура угроз и используемых ими уязвимостей, которая берется из каталогов, $p_{T_i}\left(\overline{T}_{\mathbf{X}}\right)$ — вероятность реализации угрозы T_i за время $\overline{T}_{\mathbf{X}}$, p_{V_j} — вероятность использования угрозой уязвимости V_j, $\mathbf{X}$ = {**Д, Ц, К**};
- пользуясь предложенной в работе [3] моделью оценки опасности угроз, основанной на аппарате сетей Петри.

Заключение

Анализ полученных зависимостей позволяет выявить *ряд существенных закономерностей*:

- при малых значениях вероятности нарушения доступности одной копии ИР ($\rho_{\text{Д}} < 0{,}2$) все стратегии показывают близкие результаты и практически равнозначны по показателю доступности ИР;
- при средних значениях вероятности нарушения доступности одной копии ИР ($0{,}2 < \rho_{\text{Д}} < 0{,}7$) в целом наихудшими вероятностными и наилучшими временными показателями доступности характеризуется 2-я стратегия, наилучшими вероятностными — 1-я стратегия, наихудшими временными — 4-я стратегия, а 3-я стратегия, как правило, занимает промежуточное положение;
- при больших значениях вероятности нарушения доступности одной копии ИР ($0{,}7 < \rho_{\text{Д}} < 1$) в целом наихудшими вероятностными показателями доступности характеризуется 2-я стратегия, наилучшими вероятностными и наихудшими временными — 1-я стратегия, а 3-я и 4-я стратегии, как правило, занимают промежуточное положение;
- при малых и средних значениях вероятности нарушения целостности одной копии ИР в целом наилучшими вероятностными показателями целостности характеризуется 1-я стратегия, наихудшими — 2-я стратегия, наилучшими временными — 3-я стратегия, наихудшими — 4-я стратегия;
- при больших значениях вероятности нарушения целостности одной копии ИР ($\rho_{\text{Ц}} \to 1$) в целом наилучшими вероятностными и наихудшими временными показателями целостности характеризуется 1-я стратегия, наихудшими вероятностными и наилучшими временными — 2-я стратегия, а 3-я и 4-я стратегии, как правило, занимают промежуточное положение;
- точные значения показателей доступности и целостности зависят от многих факторов: среднего времени, требуемого нарушителю для доступа к ИР при попытке нарушения информационной безопасности, вероятностей нарушения доступности и целостности одной копии ИР, распределения общего

количества экземпляров ИР между его идентичными копиями и неидентичными (предысториями), четности или нечетности числа копий и предысторий, поэтому аналитическая оценка требуемого числа копий и предысторий во многих случаях затруднительна. В связи с этим целесообразно получение численных оценок исходя из выведенных в настоящей работе аналитических зависимостей.

Приведенные в статье оценки показателей безопасности ИР распределенной вычислительной системы при различных стратегиях резервирования могут быть обобщены путем введения дополнительного предположения о том, что вероятности нарушения и (или) восстановления безопасности отдельных копий и (или) предысторий неодинаковы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Кульба В. В., Ковалевский С. С. Шелков А. Б.* Достоверность и сохранность информации в АСУ. 2-е изд. (Серия «Информационные технологии».) М.: СИНТЕГ, 2003. — 500 с.
2. *Ширяев А. Н.* Вероятность. В 2-х кн. 3-е изд. М.: МЦНМО, 2004. — 928 с.
3. *Язов Ю. К.* Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. — 274 с.