С. В. Запечников

РЕГУЛИРОВАНИЕ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В РАСПРЕДЕЛЕННОЙ КОМПЬЮТЕРНОЙ СРЕДЕ НА ОСНОВЕ ПРИМЕНЕНИЯ СТРАТЕГИИ РЕЗЕРВИРОВАНИЯ С ДРОБНОЙ КРАТНОСТЬЮ[1]

Введение

В соответствии с определением стандарта ГОСТ 7.0 – 99 под *информационным ресурсом* (ИР) понимается любая совокупность данных, организованных для эффективного получения достоверной информации. Для целей настоящей работы введем вспомогательные определения. *Информационным элементом* (ИЭ) будем называть любую минимальную однородную с точки зрения условий обеспечения информационной безопасности совокупность данных, формируемых и циркулирующих в распределенной компьютерной среде (РКС). *Информационным объектом* (ИО) будем называть совокупность взаимосвязанных ИЭ, выделяемую по функциональному или иному признаку, такую, что среди них имеется: 1) единственный ИЭ, который не может быть получен ни из каких других ИЭ информационного объекта посредством реализованных в РКС процедур обработки данных; 2) единственный ИЭ, из которого не может быть получен никакой другой ИЭ информационного объекта посредством реализованных в РКС процедур обработки данных.

Стратегией управления информационным ресурсом (СУИР) будем называть совокупность однородных в функциональном отношении алгоритмов обработки данных и протоколов обмена данными, которые предназначены для организованного управления ИЭ на протяжении его жизненного цикла посредством преобразования его в некоторый ИО.

1. Формализация стратегий управления информационными ресурсами

Формально СУИР есть комплекс из пяти алгоритмов и (или) протоколов, применяемых к некоторому ИЭ и выполнимых за конечное (практически приемлемое) время:

$S=\{Par\_Gen^S, Gen\_Distr^S, Restore^S, Regen\_Redistr^S, Del^S\}$.

В нее входят следующие алгоритмы и (или) протоколы.

1. *Алгоритм генерации начальных параметров* Par_Gen^S. Это детерминированный либо вероятностный алгоритм, исходными данными для которого служат правила политики обеспечения безопасности ИР. Алгоритм вырабатывает значения параметров ИО, необходимые для применения СУИР, например количество экземпляров ИЭ, область допустимых значений ИЭ, продолжительность периодов времени между сменой значений ИЭ и пр.

[1] Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 11-07-00268-а).

2. *Алгоритм* или *протокол генерации и распределения информационных элементов* Gen_Distr^S. Это детерминированный либо вероятностный алгоритм (протокол), на вход которого подаются параметры ИО, выработанные алгоритмом Par_Gen^S, и значение некоторого информационного элемента E_{In}, называемого *входным ИЭ*. Алгоритм (протокол) возвращает выработанные им значения множества ИЭ, задействованных в СУИР.

3. *Алгоритм* или *протокол выборки информационного элемента* Restore^S. Это детерминированный алгоритм (протокол), на вход которого подается подмножество ИЭ, порожденных алгоритмом (протоколом) Gen_Distr^S, параметры ИО, выработанные алгоритмом Par_Gen^S. Алгоритм (протокол) возвращает выработанное им значение некоторого информационного элемента E_{Out}, называемого *выходным ИЭ*.

4. *Алгоритм* или *протокол регенерации и перераспределения информационных элементов* Regen_Redistr^S. Это детерминированный либо вероятностный алгоритм, на вход которого подаются параметры ИО, выработанные алгоритмом Par_Gen^S, значения ИЭ, выработанные при вызове алгоритма (протокола) Gen_Distr^S либо при предыдущих вызовах алгоритма (протокола) Regen_Redistr^S. Алгоритм (протокол) возвращает выбранные им новые значения множества ИЭ, задействованных в СУИР.

5. *Алгоритм уничтожения информационных элементов* Del^S. Это детерминированный алгоритм, на вход которого подаются параметры ИО, выработанные алгоритмом Par_Gen^S, и значения всех ИЭ, задействованных в СУИР. Алгоритм присваивает всем ИЭ «пустые» значения, обозначаемые $\varnothing$.

Пусть $\Delta T = \langle \Delta T_1, \Delta T_2, ..., \Delta T_m \rangle$ – непрерывная последовательность временных интервалов, составляющих жизненный цикл ИО, на каждом из которых значения информационных элементов СУИР неизменны. Обозначим через `τ – момент начала интервала $\Delta T_1$; τ' – момент окончания интервала $\Delta T_m$; $\tau_i$, $i = \overline{2,m}$ – моменты окончания интервалов $\Delta T_{i-1}$ и начала интервалов $\Delta T_i$, в частности, $\tau_1$= `τ; $|\Delta T_i|$ – длина интервала ΔT_i. Алгоритм Par_Gen^S выполняется однажды перед началом применения СУИР. Алгоритм (протокол) Gen_Distr^S выполняется однажды и соответствует началу интервала ΔT_1. Алгоритм (протокол) Regen_Redistr^S выполняется $m-1$ раз и соответствует началу интервалов $\Delta T_2, ..., \Delta T_m$. Алгоритм (протокол) Del^S выполняется один раз и соответствует моменту окончания интервала ΔT_m.

Таким образом, управление информационными ресурсами посредством формирования СУИР заключается в следующем. *Объектом управления* является некоторый ИО в составе системы ИР РКС. Объект управления подвержен *внешним возмущениям* в форме порождаемых действиями злоумышленника неблагоприятных событий, приводящих к нарушениям доступности, целостности, конфиденциальности ИЭ в составе ИО. *Органом управления* является лицо, принимающее решение об использовании СУИР на этапе создания ИС с целью достижения заданных значений показателей безопасности ИР либо на этапе ее эксплуатации с целью корректировки значений показателей безопасности ИР РКС. *Управляющее воздействие* реализуется путем выбора самой СУИР и ее параметров, таких как кратность резервирования, периодичность снятия резервных копий и т. п. *Обратная связь* реализуется посредством оценки достигнутых значений вероятностных показателей безопасности ИР и (или) стоимостных показателей риска нарушения безопасности ИР и их сравнения с требуемыми или желательными значениями.

В качестве формальной конструкции для представления ИО, формируемых при использовании СУИР, удобно применить модели на основе обобщенных сетей Петри. В терминах этой модели каждый такой ИО соответствует фрагменту раскрашенной временнуй сети Петри, т. е. подсети, которая имеет точно одну начальную позицию (такую, которая не имеет входящих в нее дуг) и точно одну конечную позицию (такую, которая не имеет исходящих из

нее дуг). Начальная позиция соответствует входному ИЭ, к которому применяется СУИР, т. е. такому, который замещается на период ΔT другими ИЭ, порождаемыми из него в результате срабатывания внутренних переходов подсети. Будем называть ее *входным портом*. Обозначим входной порт СУИР S через E^S_{In}. Конечная позиция соответствует выходному ИЭ, который в течение периода ΔT используется в информационной технологии вместо входного ИЭ. Будем называть ее *выходным портом*. Обозначим выходной порт СУИР S через $E^{\mathbf{S}}_{Out}$.

Все позиции и переходы сети Петри, описывающей ИР, не входящие в рассматриваемую подсеть, назовем *внешними*. Только входной порт подсети может иметь входящие в него дуги, направленные от внешних переходов к E^S_{In}. Только выходной порт подсети может иметь исходящие из него дуги, направленные от $E^{\mathbf{S}}_{Out}$ к внешним переходам.

На основе обобщения методов и средств повышения отказо-, катастрофоустойчивости и живучести РКС представляется возможным выделить ряд типовых СУИР и дать их формальные описания. Некоторые из них — более простые — основаны только на пространственном распределении ИЭ, другие — более сложные — сочетают принципы пространственного распределения и временнуй динамики ИЭ. Далее в качестве примера будем рассматривать стратегию резервирования с дробной кратностью.

2. Определение и основные характеристики стратегии резервирования с дробной кратностью

Под кратностью резервирования в литературе по теории надежности традиционно понимают отношение числа резервных элементов к числу основных элементов устройства.

Стратегией резервирования с дробной кратностью (РДК) назовем такую СУИР, которая предполагает для заданного ИЭ создание и поддержание в течение периода ΔT множества из n информационных элементов, таких, что по набору любых не менее чем m из них, где $m \le n$, может быть восстановлено значение исходного ИЭ.

Формально данная СУИР есть совокупность

$$\text{РДК} = \{\text{Par\_Gen}^{\text{РДК}}, \text{Gen\_Distr}^{\text{РДК}}, \text{Restore}^{\text{РДК}}, \text{Regen\_Redistr}^{\text{РДК}}, \text{Del}^{\text{РДК}}\}$$

алгоритмов и протоколов, выполнимых за конечное (практически приемлемое) время, в которой:

1) $\text{Par\_Gen}^{\text{РДК}}$ — алгоритм, определяющий на основании политики обеспечения безопасности ИР тот информационный элемент $E_{In}^{\mathbf{РДК}}$, к которому должна быть применена СУИР, область его допустимых значений, а также количество n и области допустимых значений резервирующих его ИЭ $\{E^{(1)}, E^{(2)}, ..., E^{(n)}\}$;

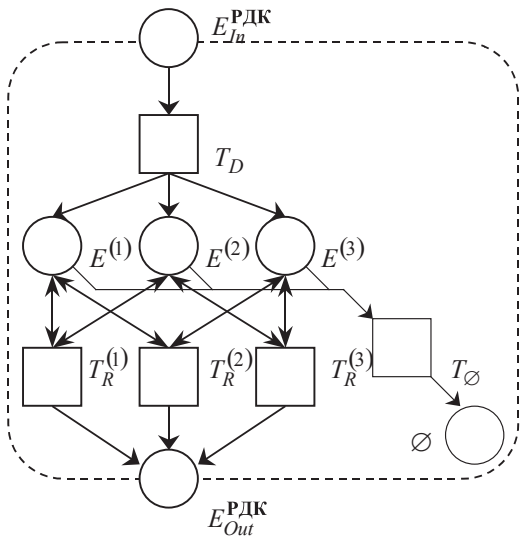
2) $\text{Gen\_Distr}^{\text{РДК}}$ — алгоритм (протокол), который по значению $e_{In}^{\mathbf{РДК}}$ входного ИЭ вычисляет, пересылает и присваивает каждому из n резервирующих его ИЭ значения $e^{(i)}$, $i = \overline{1,n}$, такие, что впоследствии значение $e_{In}^{\mathbf{РДК}}$ может быть вычислено из любого подмножества значений $\{e^{(i_1)}, e^{(i_2)}, ..., e^{(i_t)}\}$ с помощью некоторого алгоритма, в дальнейшем условно называемого алгоритмом интерполяции;

3) $\text{Restore}^{\text{РДК}}$ — алгоритм (протокол), который выбирает значения $\{e^{(i_1)}, e^{(i_2)}, ..., e^{(i_m)}\}$ одного из m-элементных подмножества $\{E^{(i_1)}, E^{(i_2)}, ..., E^{(i_m)}\}$ информационных элементов и возвращает восстановленное по ним значение выходного ИЭ: $e_{Out}^{\mathbf{РДК}}$. В случае невозможности доступа к выбранному подмножеству ИЭ берется другое подмножество ИЭ и так до тех пор, пока не будут опробованы все m-элементные подмножества резервирующих ИЭ;

4) $\text{Regen\_Redistr}^{\text{РДК}}$ — вырожденный алгоритм (формально можно считать его тождественным преобразованием всех резервирующих ИЭ);

5) $\text{Del}^{\text{РДК}}$ — алгоритм, в котором всем информационным элементам $\{E^{(1)}, E^{(2)}, ..., E^{(n)}\}$ присваиваются пустые значения: $\varnothing$.

Информационные ресурсы, формируемые при использовании СУИР РДК, описываются подсетью сети Петри, изображенной на рис. 1 (показан пример для $n = 3$, $m = 2$). Соответствие между алгоритмами и переходами сети Петри при этом следующее: выполнению алгоритма Gen_Distr^{РДК} соответствует срабатывание перехода T_D, выполнению алгоритма Restore^{РЦК} соответствует срабатывание одного из переходов $T_R^{(j)}$, $j = 1,\ldots,\binom{n}{m}$, выполнению алгоритма Del^{РЦК} – срабатывание перехода $T_\varnothing$.



Обозначения:

$E_{In}^{РДК}$ – резервируемый ИЭ (входной порт ИО, порождаемого СУИР); $E^{(i)}$, $i = 1,2,3$ – резервирующие ИЭ; $E_{Out}^{РДК}$ – ИЭ, содержащий значение, восстановленное из значений резервирующих ИЭ (выходной порт ИО, порождаемого СУИР);

T_D – переход, срабатывание которого соответствует генерации значений резервирующих ИЭ;

$T_R^{(i)}$, $i = 1,2,3$ – переходы, срабатывание которых соответствует восстановлению значения резервируемого ИЭ из значений резервирующих ИЭ;

$T_\varnothing$ – переход, срабатывание которого соответствует уничтожению значений резервирующих ИЭ.

Рис. 1. Подсеть сети Петри, моделирующая стратегию резервирования с дробной кратностью

По определению СУИР РДК преобразования, осуществляемые при срабатывании переходов T_D, $T_R^{(j)}$, $j = 1,\ldots,\binom{n}{m}$, таковы, что значения $e_{In}^{РДК}$ и $e_{Out}^{РДК}$ информационных элементов $E_{In}^{РДК}$ и $E_{Out}^{РДК}$, соответствующие маркерам одного цвета w_i в сети Петри, всегда совпадают, поэтому позиции $E_{In}^{РДК}$ и $E_{Out}^{РДК}$ на графе сети Петри, как и в предыдущей СУИР, могут быть «сшиты» в одну позицию.

Приведем примеры: стратегия резервирования ИЭ с дробной кратностью реализуется в отказоустойчивых дисковых массивах (алгоритмы RAID-5, RAID-5E [1. С. 339–344]), а также в пороговых схемах разделения секрета (СРС). Все известные пороговые СРС основаны на изоморфизме между алгебраическими структурами: $\mathbf{Z} \cong \mathbf{Z}_1 \times \mathbf{Z}_2 \times \ldots \times \mathbf{Z}_n$, где $\mathbf{Z}, \mathbf{Z}_1, \mathbf{Z}_2, \ldots, \mathbf{Z}_n$ – либо кольца целых чисел, как в СРС из [2, 3], либо кольца полиномов над конечным полем, как в СРС из [4, 5].

3. Показатели доступности ИР при применении резервирования с дробной кратностью

Исследование показателей безопасности СУИР начнем с анализа доступности. Анализ имеет целью получение для всех СУИР выражений для оценки вероятности доступности выходных ИЭ и сопоставление их с величинами, характеризующими доступность ИЭ без применения СУИР. Введем обозначения: $P^{Д}(t)$ – вероятность того, что ИЭ не утратил доступность в течение времени t без применения к нему какой-либо СУИР; $P^{S,\,Д}(t)$ – вероятность того, что выходной ИЭ не утратил доступность в течение времени t при применении стратегии S; $Q^{Д}(t) = 1 - P^{Д}(t)$ и $Q^{S,\,Д}(t) = 1 - P^{S,\,Д}(t)$ – вероятности противоположных событий; $\mu^{Д}(t)$ – интенсивность потока неблагоприятных событий (атак нарушителя), приводящих к утрате доступности ИЭ без

применения к нему какой-либо СУИР, в момент времени t; $\mu^{S,Д}(t)$ — интенсивность потока неблагоприятных событий, приводящих к утрате доступности ИЭ при применении стратегии S, в момент времени t.

Изменение показателей доступности ИЭ при применении к ним СУИР характеризуется следующими функциями: $G_P^{S,Д}(t)=\frac{P^{S,Д}(t)}{P^{Д}(t)}$ — выигрыш по вероятности сохранения доступности; $G_Q^{S,Д}(t)=\frac{Q^{S,Д}(t)}{Q^{Д}(t)}$ — выигрыш по вероятности утраты доступности; $G_\mu^{S,Д}(t)=\frac{\mu^{S,Д}(t)}{\mu^{Д}(t)}$ — выигрыш по интенсивности событий, в результате которых происходит утрата доступности ИЭ.

Анализ проводился при следующих исходных предположениях:

- в пределах одного непрерывного временного интервала все ИЭ, задействованные в СУИР, считаются невосстанавливаемыми по доступности;
- во всех практических задачах считается, что найдется такое положительное ε , что $|1-g^{S,Д}|\geq\varepsilon$, $|1-g_Q^{S,Д}|\geq\varepsilon$, $|1-g_\mu^{S,Д}|\geq\varepsilon$, где $g_P^{S,Д}=G_P^{S,Д}(t)|_t$, $g_Q^{S,Д}=G_Q^{S,Д}(t)|_t$, $g_\mu^{S,Д}=G_\mu^{S,Д}(t)|_t$;
- поток неблагоприятных событий (атак нарушителя), приводящих к утрате доступности ИЭ, простейший с интенсивностью μ (пользуясь предельной теоремой теории потоков [6. § 2.4], считаем, что при сложении n независимых стационарных ординарных потоков с интенсивностью μ каждый получается снова стационарный ординарный поток с интенсивностью $n\mu$);
- для получения верхних и нижних оценок вероятностных показателей рассматриваются наилучший и наихудший случаи соответственно: 1) суммарная интенсивность потока неблагоприятных событий до и после применения СУИР к ИЭ не изменяется; 2) после применения СУИР интенсивность потока неблагоприятных событий (атак нарушителя) для каждого ИЭ становится такой же, какой была для ИЭ до применения СУИР.

При резервировании с дробной кратностью ИЭ сохраняет доступность в течение времени t в случае утраты доступности не более чем n — μ резервирующих элементов $\{E^{(i_1)}, E^{(i_2)}, ..., E^{(i_{n-m})}\}$. Будем полагать, что во всех практических задачах вероятности утраты доступности всех резервирующих ИЭ равны.

Введем вспомогательные обозначения: пусть A — событие, заключающееся в том, что $E_{Out}^{РДК}$ доступен, A_l — событие, состоящее в утрате доступности любых l резервирующих ИЭ $\{E^{(i1)}, ..., E^{(il)}\}$, где $0\leq l\leq n$, в течение времени t. Тогда $A=\sum_{l=0}^{n-m}A_l$. Событие A_l произойдет, если доступность любых l резервирующих ИЭ будет утрачена, а остальные $n-l$ останутся доступными. Во всех практических задачах будем полагать, что вероятности утраты доступности всех резервирующих ИЭ равны. Тогда вероятность события A_l определяется по формуле Бернулли: $P(A_l)=\binom{n}{l}Q^l(t)P^{n-l}(t)$. Поскольку события A_l попарно несовместны, то

$$P^{РДК,Д}(t)=P(A)=\sum_{l=0}^{n-m}P(A_l)=\sum_{l=0}^{n-m}\binom{n}{l}Q^l(t)P^{n-l}(t).$$

Формула для $G_\mu^{РДК,Д}(t)$ выводится следующим образом: поскольку $\mu^{РДК,Д}(t)=\frac{f^{РДК}(t)}{P^{РДК,Д}(t)}$, находим $f^{РДК}(t)=-\frac{dP^{РДК,Д}}{dt}=\binom{n}{n-m}mQ^{n-m}(t)P^{m-1}(t)f(t)$, откуда

$$G_\mu^{РДК,Д}(t)=\frac{\mu^{РДК,Д}(t)}{\mu^{Д}(t)}=\frac{m}{n}\cdot\frac{\binom{n}{n-m}Q^{n-m}(t)P^m(t)}{\sum_{l=0}^{n-m}\binom{n}{l}Q^l(t)P^{n-l}(t)}.$$

Для случая, когда суммарная интенсивность неблагоприятных событий до и после применения СУИР не изменяется, получаем:

$$G_P^{\text{РДК},Д}(t)=\frac{\sum_{l=0}^{n-m}\binom{n}{l}\left(1-e^{-\mu t^{\,l}}\right)e^{-\mu(n-l)t}}{e^{-\mu nt}}, \quad (1)$$

$$G_Q^{\text{РДК},Д}(t)=\frac{1-\sum_{l=0}^{n-m}\binom{n}{l}\left(1-e^{-\mu t^{\,l}}\right)e^{-\mu(n-l)t}}{1-e^{-\mu nt}}, \quad (2)$$

$$G_\mu^{\text{РДК},Д}(t)=\frac{m}{n}\cdot\frac{\binom{n}{n-m}\left(1-e^{-\mu t}\right)^{n-m}\cdot e^{-\mu mt}}{\sum_{l=0}^{n-m}\left[\binom{n}{l}\left(1-e^{-\mu lt}\right)e^{-\mu(n-l)t}\right]}, \quad (3)$$

Если в начальный момент времени все резервирующие ИЭ доступны, то $\frac{\mu^{\text{РДК},Д}(0)}{\mu(0)}=0$. При $t\to\infty$ имеет место равенство: $=\lim_{t\to\infty}G_\mu^{\text{РДК},Д}=\frac{m}{n}$. Таким образом, применение к ИЭ рассматриваемой СУИР приводит к изменению функции выигрыша по интенсивности утраты доступности со временем от 0 до постоянной величины, равной m/n.

Случай 2 отличается тем, что в формулах (1) и (2) отсутствует n в знаменателе, а (3) умножается на множитель n.

Из анализа зависимостей следует, что использование данной стратегии выгодно в основном только в случае 1 (в случае 2 — только на очень малых временных интервалах).

4. Показатели целостности ИР при применении резервирования с дробной кратностью

Анализ показателей целостности имеет целью получение для всех СУИР выражений для оценки вероятности сохранения целостности выходных ИЭ и сопоставление их с величинами, характеризующими целостность ИЭ без применения СУИР. Введем обозначения: $P^{Ц}(t)$ — вероятность того, что ИЭ сохраняет целостность в течение времени t без применения к нему какой-либо СУИР; $P^{S,\,Ц}(t)$ — вероятность того, что выходной ИЭ сохраняет целостность в течение времени t при применении стратегии S; $Q^{Ц}(t)=1-P^{Ц}(t)$ и $Q^{S,\,Ц}(t)=1-P^{S,\,Ц}(t)$ — вероятности противоположных событий; $\mu^{Ц}(t)$ — интенсивность потока неблагоприятных событий, приводящих к утрате целостности ИЭ в момент времени t без применения к нему какой-либо СУИР; $\mu^{S,\,Ц}(t)$ — интенсивность потока неблагоприятных событий, приводящих к утрате целостности ИЭ в момент времени t при применении стратегии S.

Изменение показателей целостности ИЭ при применении к ним СУИР характеризуется следующими функциями: $G_P^{S,Ц}(t)=\frac{P^{S,Ц}(t)}{P^{Ц}(t)}$ — выигрыш по вероятности сохранения целостности; $G_Q^{S,Ц}(t)=\frac{Q^{S,Ц}(t)}{Q^{Ц}(t)}$ — выигрыш по вероятности утраты целостности; $G_\mu^{S,Ц}(t)=\frac{\mu^{S,Ц}(t)}{\mu^{Ц}(t)}$ — выигрыш по интенсив-ности событий, в результате которых происходит утрата целостности ИЭ.

Анализ проводился при следующих исходных предположениях:

- в пределах одного непрерывного временного интервала целостность всех ИЭ, задействованных в СУИР, считается невосстанавливаемой;
- во всех практических задачах считается, что найдется такое положительное ε, что $|1-g^{S,\,Ц}|\ge\varepsilon$, $|1-g_Q^{S,\,Ц}|\ge\varepsilon$, $|1-g_\mu^{S,\,Ц}|\ge\varepsilon$, где $g_\rho^{S,\,Ц}=G_\rho^{S,\,Ц}(t)\big|_t$, $g_Q^{S,\,Ц}=G_Q^{S,\,Ц}(t)\big|_t$, $g_\mu^{S,\,Ц}=G_\mu^{S,\,Ц}(t)\big|_t$;
- поток неблагоприятных событий, приводящих к утрате целостности ИЭ, простейший с интенсивностью μ;

- для получения верхних и нижних оценок вероятностных показателей рассматриваются наилучший и наихудший случаи соответственно: 1) суммарная интенсивность потока неблагоприятных событий до и после применения СУИР к ИЭ не изменяется; 2) после применения СУИР интенсивность потока неблагоприятных событий для каждого ИЭ становится такой же, какой была для ИЭ до применения СУИР.

Пусть $Q^{\text{РДК, Ц}}(t)$ — вероятность того, что при применении рассматриваемой стратегии за время t утрачена целостность выходного ИЭ $E_{Out}^{\text{РДК}}$, $Ql(t)$ — вероятность того, что за время t утрачена целостность резервирующего ИЭ $E^{(l)}$, $l=1,n$; $P^{\text{РДК, Ц}}(t)=1-Q^{\text{РДК, Ц}}(t)$, $P_l(t)=1-Q_l(t)$ — вероятности противоположных событий.

В рассматриваемой СУИР значение выходного ИЭ находится при условии доступа к любому подмножеству из m резервирующих ИЭ. Обозначим m-элементные подмножества резервирующих ИЭ $\{E^{(l_1)}, \ldots, E^{(l_m)}\}$ через B_m. В каждом конкретном случае восстановление значения выходного ИЭ может осуществляться из различных m-элементных подмножеств резервирующих ИЭ (остальные ИЭ не читаются и не контролируются). Поэтому вероятность того, что значение выходного ИЭ, прочитанное в произвольный момент времени t, не совпадает с его истинным значением, оценивается сверху и снизу величинами $\overline{Q}^{\text{РДК,Ц}}(t)=\max\limits_{B_m}\left\{1-\prod\limits_{l\in B_m}P_l(t)\right\}$ и $\underline{Q}^{\text{РДК,Ц}}(t)=\min\limits_{B_m}\left\{1-\prod\limits_{l\in B_m}P_l(t)\right\}$ соответственно.

Если вероятности утраты целостности для всех резервирующих ИЭ одинаковы, то верхняя и нижняя оценки совмещаются и $Q^{\text{РДК,Ц}}(t)=1-(P_l(t))^m$. Интенсивность нарушения целостности выходного ИЭ равна $\mu^{\text{РДК,Ц}}(t)=-\dfrac{dP^{\text{РДК,Ц}}/dt}{P^{\text{РДК,Ц}}(t)}$.

При предположении о том, что суммарная интенсивность неблагоприятных событий до и после применения СУИР не изменяется (случай 1), функции выигрыша имеют вид:

$$G_P^{\text{РДК,Ц}}(t)=\frac{e^{-\mu mt}}{e^{-\mu nt}}, \tag{4}$$

$$G_Q^{\text{РДК,Ц}}(t)=\frac{1-e^{-\mu mt}}{1-e^{-\mu nt}}, \tag{5}$$

и так как $\mu^{\text{РДК,Ц}}(t)=-\dfrac{-\mu m e^{-\mu mt}}{e^{-\mu mt}}=m\mu$, то

$$G_\mu^{\text{РДК,Ц}}(t)=\frac{m\mu}{n\mu}=\frac{m}{n}. \tag{6}$$

В случае 2 отличие состоит в том, что в (4)—(5) отсутствует n в знаменателе, а (6) умножается на множитель n, т. е. $G_\mu^{\text{РДК, Ц}}(t)=m$.

В случае 2 использование этой стратегии невыгодно, так как приводит к проигрышу по вероятностям и по интенсивности.

5. Показатели конфиденциальности ИР при применении резервирования с дробной кратностью

Анализ показателей конфиденциальности имеет целью получение для всех СУИР выражений для оценки вероятности сохранения конфиденциальности выходных ИЭ и сопоставление их с величинами, характеризующими конфиденциальность ИЭ без применения СУИР. Введем обозначения:

$P^K(t)$— вероятность того, что ИЭ сохраняет конфиденциальность в течение времени t без применения к нему какой-либо СУИР;

$P^{S,\,K}(t)$— вероятность того, что выходной ИЭ сохраняет конфиденциальность в течение времени t при применении стратегии S;

$Q^K(t) = 1-P^K(t)$ и $Q^{S,K}(t) = 1-P^{S,K}(t)$ — вероятности противоположных событий;

$\mu^{Ц}(t)$ — интенсивность потока неблагоприятных событий, приводящих к утрате конфиденциальности ИЭ в момент времени t без применения к нему какой-либо СУИР;

$\mu^{S,Ц}(t)$ — интенсивность потока неблагоприятных событий, приводящих к утрате конфиденциальности ИЭ в момент времени t при применении стратегии S.

Изменение показателей конфиденциальности ИЭ при применении к ним СУИР характеризуется следующими функциями: $G_P^{\mathbf{S},K}(t)=\frac{P^{\mathbf{S},K}(t)}{P^K(t)}$ — выигрыш по вероятности сохранения конфиденциальности; $G_Q^{\mathbf{S},K}(t)=\frac{Q^{\mathbf{S},K}(t)}{Q^K(t)}$ — выигрыш по вероятности утраты конфиденциальности; $G_\mu^{\mathbf{S},K}(t)=\frac{\mu^{\mathbf{S},K}(t)}{\mu^K(t)}$ — выигрыш по интенсивности событий, в результате которых происходит утрата конфиденциальности ИЭ.

Анализ проводился при следующих исходных предположениях:

- в пределах одного непрерывного временного интервала конфиденциальность всех ИЭ, задействованных в СУИР, считается невосстанавливаемой;
- во всех практических задачах считается, что найдется такое положительное ε, что $|1-g^{S,K}| \geq \varepsilon$, $|1-g_Q^{S,K}| \geq \varepsilon$, $|1-g_\mu^{S,K}| \geq \varepsilon$, где $g_\rho^{S,K} = G_\rho^{S,K}(t)|_t$, $g_Q^{S,K} = G_Q^{S,K}(t)|_t$, $g_\mu^{S,K} = G_\mu^{S,K}(t)|_t$;
- поток неблагоприятных событий, приводящих к утрате конфиденциальности ИЭ, простейший с интенсивностью μ;
- для получения верхних и нижних оценок вероятностных показателей рассматриваются наилучший и наихудший случаи соответственно: 1) суммарная интенсивность потока неблагоприятных событий до и после применения СУИР к ИЭ не изменяется; 2) после применения СУИР интенсивность потока неблагоприятных событий для каждого ИЭ становится такой же, какой была для ИЭ до применения СУИР.

Конфиденциальность ИЭ не является объективно фиксируемым свойством. Поэтому особенность анализа показателей конфиденциальности ИЭ заключается в том, что хотя вероятность утраты конфиденциальности зависит от длины временных интервалов, на которых ИЭ принимают определенные значения, но независимо от времени наступления этого события утрата конфиденциальности происходит на всем рассматриваемом интервале.

При применении стратегии РДК утрата конфиденциальности выходного ИЭ наступает в случае одновременной утраты конфиденциальности любого подмножества резервирующих ИЭ, состоящего из m или более элементов. Во всех практических задачах будем полагать, что вероятности утраты конфиденциальности всех резервирующих ИЭ равны. Используем те же, что и ранее, обозначения для вероятности компрометации резервирующих ИЭ: $P(t)$ и $Q(t)=1-P(t)$. Следовательно,

$$P^{\mathbf{РДК},K}(t)=\sum_{l=0}^{m-1}\binom{n}{l}Q^l(t)P^{n-l}(t) \qquad (7)$$

Функция выигрыша по интенсивности может быть найдена следующим образом. Так как плотность распределения времени до утраты конфиденциальности $f^{\mathbf{РДК}}(t)=-\frac{dP^{\mathbf{РДК},K}}{dt}$, то, используя формулу (7), получим:

$$f^{\mathbf{РДК}}(t)=-\sum_{l=0}^{m-1}\binom{n}{l}lQ^{l-1}(t)P^{n-l}(t)f(t)+\sum_{l=0}^{m-1}\binom{n}{l}(n-l)Q^l(t)P^{n-l-1}(t)f(t),$$

где $f(t)$ — как и ранее, функция плотности распределения времени до утраты конфиденциальности резервирующего ИЭ. После преобразования получаем:

$$f^{\mathbf{РДК}}(t)=(n-m+1)\binom{n}{m-1}Q^{m-1}(t)P^{n-m}(t)f(t).$$

Можно показать, что интенсивность потока событий, приводящих к утрате конфиденциальности выходного ИЭ:

$$\mu^{\text{РДК},K}(t)=\frac{f^{\text{РДК}}(t)}{P^{\text{РДК},K}(t)}=\frac{(n-m+1)\binom{n}{m-1}Q^{m-1}(t)P^{n-m-1}(t)}{\sum_{l=0}^{m-1}\binom{n}{l}Q^{l}(t)P^{n-l}(t)}\mu^{K}(t).$$

Отсюда выводится искомая функция:

$$G_{\mu}^{\text{РДК},K}(t)=\frac{\mu^{\text{РДК},K}(t)}{n\mu^{K}(t)}=\frac{n-m+1}{n}\cdot\frac{\binom{n}{m-1}Q^{m-1}(t)P^{n-m-1}(t)}{\sum_{l=0}^{m-1}\binom{n}{l}Q^{l}(t)P^{n-l}(t)}.$$

Если в начальный момент времени не утрачена конфиденциальность ИЭ, то $\mu^{\text{РДК},K}(0)/\mu^{K}(0)=0$, а

$$\lim_{t\to\infty}G_{\mu}^{\text{РДК},K}(t)=\lim_{t\to\infty}\frac{\mu_c(t)}{\mu(t)}=\frac{n-m+1}{n}\cdot\lim_{t\to\infty}\frac{1}{\sum_{l=0}^{m-1}\frac{\binom{n}{l}}{\binom{n}{m-1}}\left(\frac{P(t)}{Q(t)}\right)^{m-l-1}}=1-\frac{m-1}{n}.$$

В предположении о том, что интенсивности потоков неблагоприятных событий, приводящих к нарушению конфиденциальности резервирующих ИЭ, равны, т. е. $\mu_1=\ldots=\mu_n=\mu$, имеем:

$$P^{\text{РДК},K}(t)=\sum_{l=0}^{m-1}\binom{n}{l}\left(1-e^{-\mu t^{l}}\right)e^{-\mu(n-l)t}.$$

Считая, что суммарная интенсивность неблагоприятных событий при применении СУИР и без нее не изменяется (случай 1), получаем функции выигрыша:

$$G_{P}^{\text{РДК},K}(t)=\frac{\sum_{l=0}^{m-1}\binom{n}{l}\left(1-e^{-\mu t^{l}}\right)e^{-\mu(n-l)t}}{e^{-\mu nt}}, \tag{8}$$

$$G_{Q}^{\text{РДК},K}(t)=\frac{1-\sum_{l=0}^{m-1}\binom{n}{l}\left(1-e^{-\mu t^{l}}\right)e^{-\mu(n-l)t}}{1-e^{-\mu nt}}, \tag{9}$$

$$G_{\mu}^{\text{РДК},K}(t)=\left(1-\frac{m-1}{n}\right)\cdot\binom{n}{m-1}\cdot\frac{\left(1-e^{-\mu t}\right)^{m-1}e^{-\mu(n-m-1)t}}{\sum_{l=0}^{m-1}\binom{n}{l}\left(1-e^{-\mu t^{l}}\right)e^{-\mu(n-l)t}}. \tag{10}$$

Случай 2 отличается тем, что в формулах (8) и (9) отсутствует n в знаменателе, а (10) умножается на множитель n.

Заключение

Введенное понятие СУИР и способ модельного представления СУИР позволяют формализовать типовые приемы использования элементов и массивов данных в РКС и исследовать влияние этих стратегий на доступность, целостность и конфиденциальность информации, обрабатываемой, передаваемой и хранимой в РКС.

Обнаруженные закономерности изменения показателей доступности, целостности и конфиденциальности ИР при применении СУИР позволили выявить СУИР, применение которых рационально в смысле повышения показателей доступности, целостности и конфиденциальности информационных ресурсов, а также определить условия их рационального применения. Одной из таких СУИР является стратегия резервирования с дробной кратностью. В отличие от традиционных стратегий резервирования ИР с целой кратностью, т. е. путем создания множества идентичных

копий ИР (дублирования, троирования и т. д.), улучшающих показатели доступности, улучшающих или не изменяющих показатели целостности, но ухудшающих показатели конфиденциальности, данная стратегия позволяет достичь сбалансированных значений показателей доступности, целостности и конфиденциальности. По этой причине стратегию резервирования с дробной кратностью можно рекомендовать в качестве основы реализации средств обеспечения безопасности ИР в условиях частичного разрушения РКС.

СПИСОК ЛИТЕРАТУРЫ:

1. *Таненбаум Э., ван Стеен М.* Распределенные системы. Принципы и парадигмы. СПб.: Питер, 2003. — 877 с. (Серия «Классика computer science»).
2. *De Santis A. [и др.]* How to share a function securely // Proc. of ACM 26th Annual symposium on the Theory of computing. ACM. 1994. P. 522—533.
3. *Iftene S.* Compartmented Secret Sharing Based on the Chinese Remainder Theorem. URL: http://eprint.iacr.org/2005/408.
4. *Blakley B.* Safeguarding cryptographic keys // Proc. of the USA National Computer Conf. 1979. American Federation of Information Processing Societies Proceedings. Vol. 48. P. 313—317.
5. *Shamir A.* How to share a secret // Comm. of the ACM. 1979. № 22. P. 612—613.
6. *Вентцель Е. С., Овчаров Л. А.* Теория случайных процессов и ее инженерные приложения: учеб. пособие для втузов. 2-е изд., стер. М.: Высш. шк., 2000. — 383 с.