П. 6 Комплекс моделей опасных воздействий на защищаемую систему

ИС полагается защищенной от опасных программно-технических воздействий в течение заданного периода времени $T_{зад}$, если к началу периода целостность системы обеспечена и в течение всего периода $T_{зад}$ либо источники опасности не проникают в систему, либо не происходит их активизации.

П.6.1 Технология 1. Профилактическая диагностика целостности системы

Технология 1 основана на профилактической диагностике целостности системы (описание см. в разделе 2). Некоторые из моделируемых случаев соотношения между периодами диагностики, заданным временем безопасного функционирования, временем проникновения и активизации источников опасности отображены на рис. П.6.1.

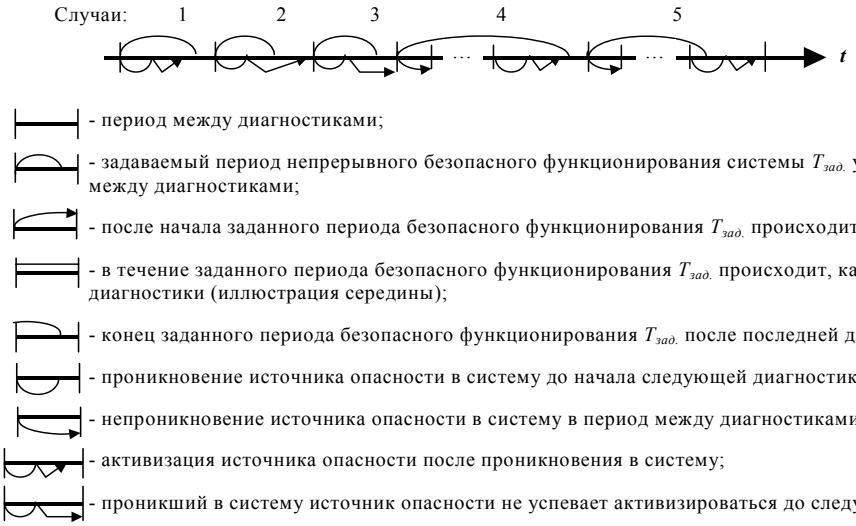

Рис. П.6.1. Иллюстрация формальных процессов защиты от опасных воздействий на основе профилактической диагностики целостности системы

Случаи 1, 4 характеризуют воздействие проникших источников опасности в течение заданного периода безопасного функционирования системы $T_{зад.}$. Случаи 2, 3, 5 – безопасное функционирование системы в течение периода $T_{зад.}$.

Возможны варианты:

вариант 1 – заданный период безопасного функционирования $T_{зад.}$ меньше периода между диагностиками ($T_{зад.} < T_{меж.} + T_{диаг.}$), т.е. $T_{зад.}$ либо укладывается между диагностиками, либо за это время может произойти лишь одна диагностика;

вариант 2 – заданный период безопасного функционирования $T_{зад.}$ больше или равен периоду между диагностиками ($T_{зад.} \geq T_{меж.} + T_{диаг.}$), т.е. за это время заведомо произойдет одна или более диагностик.

Здесь $T_{меж.}$ – время с момента завершения предыдущей диагностики (завершенной, при необходимости, восстановлением целостности системы) до начала следующей диагностики согласно регламенту, $T_{диаг.}$ – время диагностики, $T_{зад.}$ – задаваемый период непрерывного безопасного функционирования системы. В инструментариях $T_{меж.}$, $T_{диаг.}$, $T_{зад.}$ полагаются постоянными величинами (неслучайными).

Утверждение П.6.1. Для варианта 1 при условии независимости исходных характеристик вероятность $P_{возд.(1)}(T_{зад.})$ отсутствия опасного воздействия в течение периода $T_{зад.}$:

$$P_{возд.(1)}(T_{зад.}) = 1 - \Omega_{возд.} * \Omega_{акт.}(T_{зад.}), \qquad (П.6.1)$$

где * – знак свертки;

$\Omega_{возд.}(t)$ – ФР времени между воздействиями на систему с целью внедрения источника опасности, в КОК $\Omega_{возд.}(t)=1-exp(-\sigma t)$, σ – частота воздействий;

$\Omega_{акт.}(t)$ – ФР времени активизации источника опасности после его проникновения в систему, в инструментариях $\Omega_{акт.}(t) = 1-exp(-t/\beta)$, β – среднее время активизации проникшего в систему источника опасности.

Примечание. Эта же формула используется для оценки вероятности отсутствия опасных воздействий без какой-либо диагностики в предположении, что к началу периода $T_{зад.}$ целостность системы обеспечена (расчет по формуле (П.6.1) для любых значений $T_{зад.}$).

Доказательство. Поскольку в период между диагностиками система практически не защищена от проникновений, то опасное воздействие за период $T_{зад.}$ состоит в том, что источник опасности не только проникнет в систему (вероятность чего $\Omega_{возд.}(T_{зад.})$), но и успеет активизироваться (общая вероятность с учетом независимости равна $\Omega_{возд.} * \Omega_{акт.}(T_{зад.})$). Искомая вероятность является дополнением до единицы.

Доказательство Утверждения П.6.1 завершено.

Замечание. Вероятность $P_{нач.}$ того, что за начальный период $T_{зад.}$ до первой диагностики опасных воздействий не было, также равна $P_{возд.(1)}(T_{зад.})$. Этому же равна и вероятность $P_{кон.}$ отсутствия опасных воздействий после последней диагностики.

Утверждение П.6.2. Для варианта 2 при условии независимости исходных характеристик вероятность отсутствия опасного воздействия в течение периода $T_{зад.}$:

$$P_{возд.(2)} = \frac{N(T_{меж.} + T_{диаг.})}{T_{зад.}} \cdot P_{возд.(1)}{}^{N}(T_{меж.} + T_{диаг.}) + \frac{T_{ост.}}{T_{зад.}} P_{возд.(1)}(T_{ост.}), \qquad (П.6.2)$$

где $N = \lfloor T_{зад.}/(T_{меж.} + T_{диаг.}) \rfloor$ – целая часть, $T_{ост.} = T_{зад.} - N(T_{меж.} + T_{диаг.})$.

Доказательство. С учетом независимости периодов между диагностиками (т.к. в результате диагностики происходит полное восстановление целостности системы):

$$P_{возд.(2)} = P_{серед.} + P_{кон.}, \qquad (П.6.3)$$

где $P_{серед.}$ – вероятность отсутствия опасного воздействия в течение всех периодов между диагностиками, целиком вошедшими в $T_{зад.}$. Определяя долю этих периодов $\frac{N(T_{меж.}+T_{диаг.})}{T_{зад.}}$ в общем заданном периоде $T_{зад.}$ имеем

$$P_{серед.}=\frac{N(T_{меж.}+T_{диаг.})}{T_{зад.}}\cdot P_{цел.(1)}{}^{N};$$

$P_{цел.(1)}$ – вероятность того, что источники опасности не будут воздействовать за один период между диагностиками, целиком вошедший в пределы времени $T_{зад.}$,

$P_{цел.(1)} = P_{возд.(1)}(T_{меж.}+ T_{диаг.})$ с расчетом по формуле (П.6.1);

$P_{кон.}$ – вероятность отсутствия опасного воздействия после последней диагностики (в конце $T_{зад.}$). С учетом доли остатка $T_{ост.}= T_{зад.}-N(T_{меж.}+T_{диаг.})$ в общем заданном периоде $T_{зад.}$ и независимости характеристик

$$P_{кон.}=\frac{T_{ост.}}{T_{зад.}}\cdot P_{возд.(1)}(T_{ост.});$$

N – число периодов между диагностиками, которые целиком вошли в пределы времени $T_{зад.}$, с округлением до целого числа $N=\lfloor T_{зад.}/(T_{меж.}+T_{диаг.})\rfloor$ – целая часть;

$P_{возд.(1)}(T_{ост.})$ – см. определение $P_{возд.(1)}(T_{зад.})$, рассчитывается по формуле (П.6.1) для остатка $T_{ост.}$, для которого выполняется условие варианта 1: $T_{ост.}<T_{меж.}+T_{диаг.}$.

Подставляя все в (П.6.3), получаем выражение, приведенное в утверждении. Тем самым *утверждение П.6.2 доказано*.

Замечание. Вероятность $P_{нач.}=P_{цел.(1)}$, $P_{серед.}$, $P_{кон.}$- вычисляются по формулам, приведенным в доказательстве.

П.6.2 Технология 2. Многосменный мониторинг безопасности

В отличие от предыдущей технология 2 подразумевает, что целостность ИС в период между диагностиками отслеживают сменяющие друг друга операторы. При обнаружении проникновения источника опасности полагается, что оператор ликвидирует его, восстанавливая целостность системы (см. в раздел 2).

Возможны варианты:

вариант 1 – заданный период безопасного функционирования $T_{зад.}$ меньше длительности работы оператора в течение одной смены ($(T_{меж.}+T_{диаг.})/k > T_{зад.}$, где k – количество смен операторов между моментами начала соседних диагностик);

вариант 2 – заданный период безопасного функционирования $T_{зад.}$ больше или равен длительности работы одного оператора, но меньше периода между диагностиками, т.е. $(T_{меж.}+T_{диаг.})/k \le T_{зад.} \le T_{меж.}+T_{диаг.}$;

вариант 3: $T_{меж.}+T_{диаг.} < T_{зад.}$, т.е. в течение заданного периода безопасного функционирования $T_{зад.}$ завершится хотя бы одна диагностика.

Утверждение П.6.3. Для варианта 1 при условии независимости исходных характеристик вероятность $P_{прон.(1)}(T_{зад.})$ отсутствия источника опасности в системе за заданный период $T_{зад.}$:

$$P_{прон.(1)}(T_{зад.})=1-\int_0^{T_{зад.}} dA(\tau)\,\Omega_{возд.}(T_{зад.}-\tau), \qquad \text{(П.6.4)}$$

где k – количество смен операторов между диагностиками;

$(T_{меж.}+T_{диаг.})/k$ – длительность работы оператора в течение смены;

$A(t)$ – ФР времени наработки оператора на ошибку (2-го рода), $T_{нар.}$ – среднее, $A(t)=1-e^{-t/Tнар.}$.

Доказательство. Наличие источника опасности в системе будет тогда, когда до завершения $T_{зад.}$ истечет время наработки оператора на ошибку (вероятность чего $\int_0^{T_{зад.}} dA(\tau)$) и в оставшееся время с момента τ до завершения $T_{зад.}$ осуществится опасное воздействие на систему (вероятность чего равна $\Omega_{возд.}(T_{зад.}-\tau)$). Дополнение этой вероятности до единицы даст искомую. *Доказательство утверждения П.6.3 завершено*.

Замечание. Вероятность $P_{нач.}$ того, что за первую рабочую смену источники опасности не проникли, равна вероятности $P_{кон.}$ того, что они не проникли и за последнюю рабочую смену, т.к. первая и последняя смены совпадают, т.е. $P_{нач.} = P_{кон.} = P_{прон.(1)}$.

Утверждение П.6.4. Для варианта 2 при условии независимости исходных характеристик вероятность отсутствия источника опасности в системе за время $T_{зад.}$ равна

$$P_{прон.(2)}(T_{зад.})=\frac{L(T_{меж.}+T_{диаг.})/k}{T_{зад.}}\cdot P_{прон.(1)}{}^{L}\left(\frac{T_{меж.}+T_{диаг.}}{k}\right)+\frac{T_{ост.(2)}}{T_{зад.}}P_{прон.(1)}(T_{ост.(2)}), \qquad \text{(П.6.5)}$$

где $L=\lfloor T_{зад.}\cdot k/(T_{меж.}+T_{диаг.})\rfloor$ – целая часть, $T_{ост.(2)} = T_{зад.} – L(T_{меж.}+ T_{диаг.})/k$.

Доказательство. С учетом независимости периодов между диагностиками (т.к. в результате диагностики происходит полное восстановление целостности системы):

$$P_{прон.(2)} = P_{серед.(2)} + P_{кон.(2)}, \qquad \text{(П.6.6)}$$

где $P_{серед.(2)}$ – вероятность того, что источники опасности не проникнут в систему за все L рабочих смен операторов, целиком вошедших в пределы времени $T_{зад.}$. Определяя долю этих смен $\frac{L(T_{меж.}+T_{диаг.})/k}{T_{зад.}}$ в общем периоде $T_{зад.}$ имеем

$$P_{серед.(2)}=\frac{L(T_{меж.}+T_{диаг.})/k}{T_{зад.}}\cdot P_{цел.(2)}^{L},$$

где $P_{цел.(2)}$ – вероятность того, что источники опасности не проникнут за одну рабочую смену операторов, целиком вошедшую в пределы времени $T_{зад.}$:

$$P_{цел.(2)} = P_{прон.(1)}((T_{меж.}+T_{диаг.})/k);$$

возведение в степень L означает событие, когда и за 1-ю, и за 2-ю, … и за L-ю смену источники опасности в систему не проникнут;

$P_{кон.(2)}$ – вероятность того, что источники опасности не проникнут в систему за последнюю рабочую смену:

$$P_{кон.(2)}=\frac{T_{ост.(2)}}{T_{зад.}}\cdot P_{прон.(1)}(T_{ост.(2)}).$$

$P_{прон.(1)}$ $(T_{ост.(2)})$ – см. определение $P_{прон.(1)}(T_{зад.})$, рассчитывается, как для варианта 1, но не для всего времени $T_{зад.}$, а для остатка $T_{ост.} = T_{зад.} - L \cdot (T_{меж.} + T_{диаг.})/k$, для которого выполняется условие варианта 1: $T_{ост.(2)} < (T_{меж.} + T_{диаг.})/k$.

Подставляя полученные выражения в (П.6.6), в итоге получаем доказываемое (П.6.5). *Доказательство утверждения П.6.5 завершено.*

Утверждение П.6.5. Для варианта 3 при условии независимости исходных характеристик вероятность отсутствия источника опасности в системе за время $T_{зад.}$ равна:

$$P_{прон.(3)} = \frac{N(T_{меж.} + T_{диаг.})}{T_{зад.}} \cdot P^{N}_{прон.(3)}(T_{меж.} + T_{диаг.}) + \frac{T_{ост.(3)}}{T_{зад.}} P_{прон.(x)}(T_{ост.(3)}), \qquad (П.6.7)$$

где $N = \lfloor T_{зад.}/(T_{меж.} + T_{диаг.}) \rfloor$ – число периодов между диагностиками, целиком вошедших в $T_{зад.}$;

$T_{ост.(3)} = T_{зад.} - N(T_{меж.} + T_{диаг.})$;

$$x = \begin{cases} 1, & если \quad T_{ост.(3)} < (T_{меж.} + T_{диаг.})/k; \\ 2, & в \quad противном \quad случае. \end{cases}$$

Доказательство. С учетом независимости периодов между диагностиками аналогично предыдущим доказательствам:

$$P_{прон.(3)}(T_{зад.}) = P_{серед.(3)} + P_{кон.(3)}, \qquad (П.6.8)$$

где $P_{серед.(3)} = \frac{N(T_{меж.} + T_{диаг.})}{T_{зад.}} \cdot P^{N}_{прон.(2)}(T_{меж.} + T_{диаг.})$, возведение в степень N означает, что источники опасности будут отсутствовать на каждом из этих N периодов;

$T_{ост.(3)}$ – это остаток времени после завершения последней диагностики до завершения периода $T_{зад.}$;

$$P_{кон.(3)} = \frac{T_{ост.(3)}}{T_{зад.}} \cdot P_{прон.(x)}(T_{ост.(3)}).$$

Подстановка полученных выражений в (П.6.8) приводит к доказываемому выражению (П.6.7).

Доказательство утверждения П.6.5 завершено.

П.6.3 Технология 3. Мониторинг безопасности с диагностикой целостности системы при каждой смене операторов

Технология 3 является частным случаем технологии 2, когда при каждой смене операторов осуществляется комплексная диагностика. Осуществляемый при этом мониторинг безопасности характеризуется контролем целостности при каждой смене оператора, что способствует повышению уровня безопасности функционирования системы по сравнению с самостоятельным использованием каждой из комбинируемых технологий.

Возможны варианты:

вариант 1 – заданный период безопасного функционирования $T_{зад.}$ меньше периода между диагностиками ($T_{зад.} < T_{меж.} + T_{диаг.}$), т.е. $T_{зад.}$ либо укладывается между диагностиками, либо в течение него может произойти лишь одна диагностика;

вариант 2 – заданный период безопасного функционирования $T_{зад.}$ больше или равен периоду между диагностиками ($T_{зад.} \geq T_{меж.} + T_{диаг.}$), т.е. за это время заведомо произойдет одна или более диагностик.

Утверждение П.6.6. Для варианта 1 вероятность $P_{возд.(1)}(T_{зад.})$ отсутствия опасных воздействий в течение периода $T_{зад.}$ при независимости исходных характеристик равна:

$$P_{возд.(1)}(T_{зад.}) = 1 - \int_{0}^{T_{зад.}} dA(\tau) \int_{0}^{T_{зад.}-\tau} d\,\Omega_{возд.} * \Omega_{акт.}(\theta). \qquad (П.6.9)$$

Доказательство. Опасное воздействие в системе произойдет лишь тогда, когда до завершения времени $T_{зад.}$ истечет время наработки оператора на ошибку (вероятность чего $\int_{0}^{T_{зад.}} dA(\tau)$), а в оставшееся время с момента τ до завершения $T_{зад.}$ осуществится не только опасное проникновение источника опасности, но и его активизация (вероятность чего $\int_{0}^{T_{зад.}-\tau} d\,\Omega_{возд.} * \Omega_{акт.}(\theta)$). Дополнение этой вероятности до единицы даст искомую. *Доказательство утверждения П.6.6 завершено.*

Замечание. Вероятность $P_{нач.}$ того, что за первую рабочую смену опасные воздействия будут отсутствовать, равна вероятности $P_{кон.}$ того, что и за последнюю рабочую смену опасных воздействий не было (т.к. была всего одна рабочая смена), т.е. $P_{нач.} = P_{кон.} = P_{возд.(1)}$.

Утверждение П.6.7. Для варианта 2 при условии независимости исходных характеристик вероятность отсутствия опасного воздействия в течение периода $T_{зад.}$ равна:

$$P_{возд.(2)}(T_{зад.}) = \frac{N(T_{меж.} + T_{диаг.})}{T_{зад.}} \cdot P^{N}_{возд.(1)}(T_{меж.} + T_{диаг.}) + \frac{T_{ост.}}{T_{зад.}} P_{возд.(1)}(T_{ост.}), \qquad (П.6.10)$$

где $N = \lfloor T_{зад.}/(T_{меж.} + T_{диаг.}) \rfloor$ – целая часть, $T_{ост.} = T_{зад.} - N(T_{меж.} + T_{диаг.})$.

Доказательство. Доказательство полностью аналогично предыдущим. С учетом независимости периодов между диагностиками

$$P_{возд.(2)}(T_{зад.}) = P_{серед.} + P_{кон.}, \qquad (П.6.11)$$

где $P_{серед.}$ – вероятность отсутствия опасных воздействий за все N рабочих смен операторов, целиком вошедших в пределы времени $T_{зад.}$:

$$P_{серед.} = \frac{N(T_{меж.} + T_{диаг.})}{T_{зад.}} \cdot P^{N}_{возд.(1)}(T_{меж.} + T_{диаг.});$$

$P_{кон.}$ – вероятность того, что опасных воздействий не произойдет за последнюю рабочую смену:

$$P_{кон.} = \frac{T_{ост.}}{T_{зад.}} \cdot P_{возд.(1)}(T_{ост.}).$$

$P_{возд.(1)}$ $(T_{ост.})$ – см. определение $P_{возд.(1)}(T_{зад.})$, рассчитывается, как для варианта 1, но не для всего времени $T_{зад.}$, а для остатка $T_{ост.} = T_{зад.} - N(T_{меж.} + T_{диаг.})$, для которого выполняется условие варианта 1: $T_{ост.} < T_{меж.} + T_{диаг.}$.

Подставляя все выражения в (П.6.11), получаем доказываемое выражение (П.6.10). *Доказательство утверждения П.6.7 завершено.*

Замечание. Для первого периода $P_{нач.} = P_{возд.(1)}(T_{меж.}+T_{диаг.})$.

Явные аналитические формулы, реализованные в инструментальных комплексах, описанных в монографии, получаются на основе интегрирования обычными методами выражений (П.6.1), (П.6.4), (П.6.9), (П.6.11) и использования результатов утверждений П.6.1-П.6.7.

Необходимые для моделирования пределы исходных значений $T_{зад}$, σ, β задаются в ТЗ или в постановках функциональных задач при указании сценариев возможного опасного воздействия, значение $T_{диаг}$ устанавливают в результате натурных экспериментов, а значение $T_{меж.}$ указывают в эксплуатационной документации.