УДК 623.618

Р.Н. Акиншин, А.А. Бирюков, И.Н. Ефремов, А.А. Буравлев

МОДЕЛИ ОПАСНЫХ ВОЗДЕЙСТВИЙ НА ЗАЩИЩАЕМУЮ ИНФОРМАЦИОННУЮ СИСТЕМУ

Предложена математическая модель оценки вероятностных параметров безопасности информации в условиях возможной реализации опасных воздействий на защищаемую систему.

Введение. Информационная система (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 [1].

Для обеспечения требуемого уровня защищенности системы возможно применение следующих технологий [1,2]:

1. Профилактическая диагностика целостности системы;
2. Многосменный мониторинг безопасности;
3. Мониторинг безопасности с диагностикой целостности системы при каждой смене операторов.

Теоретические исследования. Введем следующие обозначения: σ - частота воздействия на систему, осуществляемого с целью внедрения источника опасности; β - среднее время активизации проникшего в систему источника опасности; $T_{меж}$ - время между окончанием предыдущей и началом очередной диагностики целостности системы; $T_{диаг}$ - длительность диагностики, включая восстановление целостности системы; $T_{нар}$ - среднее время наработки оператора на ошибку; k - количество смен операторов между соседними диагностиками; $P_{зад}$ - минимально допустимая вероятность безопасного функционирования системы в течение периода $T_{зад}$.

Необходимые пределы исходных значений $T_{зад}$, σ, β задаются в техническом задании или в постановках функциональных задач при указании сценариев возможного опасного воздействия, значение $T_{диаг}$, $T_{нар}$ устанавливают в результате натурных экспериментов (для конкретного образца указывается свойственный ему способ получения или выявления характерных значений исходных данных), а значения $T_{меж}$, k указывают в эксплуатационной документации.

Технология 1. *Профилактическая диагностика целостности системы*

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.

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, но и успеет активизироваться. Таким образом, для варианта 1 при условии независимости исходных характеристик вероятность $P_{возд.}(1)(T_{зад.})$ отсутствия опасного воздействия в течение периода $T_{зад.}$:

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

где * - знак свертки; $\Omega_{возд.}(t)$ – функция распределения времени между воздействиями на систему с целью внедрения источника опасности, в КОК [1];

$\Omega_{возд.}(t)=1-exp(-\sigma t)$; $\Omega_{акт.}(t)$ - функция распределения времени активизации источника опасности после его проникновения в систему, $\Omega_{акт.}(t) = 1-exp(-t/\beta)$.

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

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

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

$$P_{серед.} = \frac{N(T_{межс.} + T_{диаг.})}{T_{зад.}} \times P_{цел.(1)}{}^{N},$$

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

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

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

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

где N – число периодов между диагностиками, которые целиком вошли в пределы времени $T_{зад.}$, с округлением до целого числа $N=[\ T_{зад.}/(T_{межс.}+T_{диаг.})]$ - целая часть.

Подставляя все в (2), получаем для варианта 2 при условии независимости исходных характеристик вероятность отсутствия опасного воздействия в течение периода $T_{зад.}$:

$$P_{возд.(2)} = \frac{N(T_{межс.} + T_{диаг.})}{T_{зад.}} \times P_{возд.(1)}{}^{N}(T_{межс.} + T_{диаг.}) + \\ + \frac{T_{ост.}}{T_{зад.}} P_{возд.(1)}(T_{ост.}) \qquad (3)$$

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.

Возможны варианты:

– вариант 1 - заданный период безопасного функционирования $T_{зад.}$ меньше длительности работы оператора в течение одной смены ($(T_{межс.}+ T_{диаг.})/k > T_{зад.}$, 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. $(T_{межс.}+T_{диаг.})/k \le T_{зад.} \le T_{межс.}+T_{диаг.}$;

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

Наличие источника опасности в системе будет тогда, когда до завершения $T_{зад.}$ истечет время наработки оператора на ошибку (вероятность чего $\int_0^{T_{зад.}} dA(\tau)$, $A(t)$ – функция распределения времени наработки оператора на ошибку (2-го рода) $A(t)=1-e^{-t/Tнар}$) и в оставшееся время с момента τ до завершения $T_{зад.}$ осуществится опасное воздействие на систему (вероятность чего равна $\Omega_{возд.}(T_{зад.} - \tau)$), тогда для варианта 1 при условии независимости исходных характеристик вероятность $P_{прон.}(T_{зад.})$ отсутствия источника опасности в системе за заданный период $T_{зад.}$:

$$P_{прон.(1)}(T_{зад.}) = 1 - \int_0^{T_{зад.}} dA(\tau)\,\Omega_{возд.}(T_{зад.} - \tau) \qquad (4)$$

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

$$P_{прон.(2)} = P_{серед.(2)} + P_{кон.(2)} \qquad (5)$$

где $P_{серед.(2)}$ - вероятность того, что источники опасности не проникнут в систему за все L ($L=[T_{зад.}\cdot k/(T_{межс.}+T_{диаг.})]$) рабочих смен операторов, целиком вошедших в пределы времени $T_{зад.}$.

Определяя долю этих смен $\frac{L(T_{межс.} + T_{диаг.})/k}{T_{зад.}}$ в общем периоде $T_{зад.}$ имеем

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

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

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

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:

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

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

Подставляя полученные выражения в (5), в итоге получаем для варианта 2 вероятность отсутствия источника опасности в системе за время $T_{зад.}$:

$$P_{прон.(2)}(T_{зад.}) = \frac{L(T_{межс.} + T_{диаг.})/k}{T_{зад.}} \times \\ \times P_{прон.(1)}{}^{L}\left(\frac{T_{межс.} + T_{диаг.}}{k}\right) + \frac{T_{ост.(2)}}{T_{зад.}} P_{прон.(1)}(T_{ост.(2)}). \qquad (6)$$

С учетом независимости периодов между диагностиками аналогично предыдущему получим:

$$P_{прон.(3)}(T_{зад.}) = P_{серед.(3)} + P_{кон.(3)}, \quad (7)$$

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 $T_{зад}$:

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

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

Подстановка полученных выражений в (7) приводит для варианта 3 вероятность отсутствия источника опасности в системе за время $T_{зад.}$ равна:

$$P_{прон.(3)} = \frac{N(T_{меж.} + T_{диаг.})}{T_{зад.}} \times \\ \times P^{N}_{прон.(3)}(T_{меж.} + T_{диаг.}) + \frac{T_{ост.(3)}}{T_{зад.}} P_{прон.(x)}(T_{ост.(3)}), \quad (8)$$

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

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

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

Осуществляемый 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.

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 $\int_0^{T_{зад.}-\tau} d\,\Omega_{возд.} * \Omega_{акт.}(\theta)$). Тогда, для варианта 1 вероятность $P_{возд.(1)}(T_{зад.})$ отсутствия опасных воздействий в течение периода $T_{зад.}$:

$$P_{возд.(1)}(T_{зад.}) = 1 - \\ - \int_0^{T_{зад.}} dA(\tau) \int_0^{T_{зад.}-\tau} d\,\Omega_{возд.} * \Omega_{акт.}(\theta). \quad (9)$$

С учетом независимости периодов между диагностиками

$$P_{возд.(2)}(T_{зад.}) = P_{серед.} + P_{кон.}, \quad (10)$$

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

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

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

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

где $P_{возд.(1)}(T_{ост.})$ – 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 (10), получаем для варианта 2 вероятность отсутствия опасного воздействия $P_{возд.(2)}(T_{зад.})$ в течение периода $T_{зад.}$:

$$P_{возд.(2)}(T_{зад.}) = \frac{N(T_{меж.} + T_{диаг.})}{T_{зад.}} \times \\ \times P^{N}_{возд.(1)}(T_{меж.} + T_{диаг.}) + \frac{T_{ост.}}{T_{зад.}} P_{возд.(1)}(T_{ост.}). \quad (11)$$

Заключение. Таким образом, в статье предложены процедуры расчета следующих величин:

– вероятность отсутствия источника опасности в системе в течение заданного периода, $P_{источн.}=P_{прон.}$ (по модели для технологии 2);

– риск необнаружения источника опасности в системе в течение заданного периода $R_{источн.}= 1 - P_{источн.}$;

– вероятность безопасного функционирования системы в течение заданного периода $P=P_{возд.}$ (по модели для технологий 1 и 3);

– риск невыполнения требований заказчика к обеспечению целостности системы в течение заданного периода $R = 1 - P$.

Данные значения могут быть использованы для определения параметров системы информационной безопасности как на этапе ее построения, так и на этапах ее эксплуатации.

Библиографический список

1. *Бескоровайный М.М., Костогрызов А.И., Львов В.М.* Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КОК»: Руководство системного аналитика. - М.: Вооружение. Политика. Конверсия, 2001- 303 с.

2. *Костогрызов А.И., Липаев В.В.* Сертификация качества функционирования автоматизированных информационных систем.- М.: Вооружение. Политика. Конверсия, 1996 - 280 с.