ПОРТФЕЛЬ РЕДАКЦИИ

БИТ

Д. А. Багаев, Ю. Н. Лаврухин, С. В. Скрыль

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ИХ ЗАЩИЩЕННОСТИ В СИСТЕМАХ РЕАЛЬНОГО ВРЕМЕНИ

Существующие тенденции широкого внедрения систем управления процессами в режиме реального времени (системы реального времени — СРВ) в сферу критических приложений наряду с неоспоримыми преимуществами порождают и ряд проблем, среди которых одной из основных является обеспечение информационной безопасности такого рода систем.

То обстоятельство, что информационные процессы в СРВ крайне критичны к своим временным параметрам, воздействие угроз информационной безопасности приводят к серьезным последствиям, связанным с огромными временными издержками по восстановлению корректности информационных процессов, подвергнутых воздействию. С учетом постоянно возрастающих требований к оперативности обработки информации в таких системах проблема обеспечения их информационной безопасности стоит в настоящее время крайне остро. При этом конфиденциальный характер информации сферы критических приложений усиливает эту тенденцию.

Необходимость адекватных угрозам информационной безопасности и особенностям функционирования СРВ мер защиты информации привела к разработке соответствующих механизмов защиты, которые в литературе известны как встраиваемые [1].

Это обусловливает необходимость рассмотрения, в качестве базовых, временных параметров СРВ как характеристики эффективности реализуемых этими системами информационных процессов и их защищенности от воздействия угроз информационной безопасности.

С целью определения формы показателя эффективности информационных процессов в СРВ условимся использовать время $\tau_{(ип)}$ реализации этих процессов и его максимально допустимое значение $\tau_{(доп)}$. При этом под временем $\tau_{(ип)}$ реализации информационных процессов в СРВ будем понимать время реализации схемы обработки информации, циркулирующей в СРВ с момента получения данных или команд на обработку до момента выдачи обработанных данных. Информационные процессы в СРВ считаются реализованными эффективно, если время $\tau_{(ип)}$ не превышает $\tau_{(доп)}$, т. е. при выполнении неравенства:

$$\tau_{(ип)} \le \tau_{(доп)}. \qquad (1)$$

Исходя из того, что входящие в данное неравенство величины являются случайными, а его выполнение является случайным событием, условие (1) опишем соответствующей вероятностью. Данная вероятность представляет собой среднее количество своевременно реализованных запросов на обработку данных в СРВ относительно их общего числа на k-м, $k = 1, 2, \ldots, K$, временном интервале $[t_{(н)k}, t_{(о)\,k}]$ функционирования СРВ:

$$P_k(\tau_{(\text{ип})k} \le \tau_{(\text{доп})k}) = \frac{1}{L_k}\sum_{l=1}^{L_k}\psi_{k,l},$$

где $\psi_{k,l} = \begin{cases} 0, & \text{если } \tau_{(\text{ип})k,l} \le \tau_{(\text{доп})k,l} \\ 1, & \text{в противном случае} \end{cases}$;

$\tau_{(\text{ип})k,\,l}$ — время реализации информационных процессов в СРВ по l-му запросу на временном интервале $[t_{(\text{н})k}, t_{(\text{о})\,k}]$;

$\tau_{(\text{доп})k,\,l}$ — максимально допустимое время реализации информационных процессов в СРВ, инициированных l-м запросом на рассматриваемом временном интервале;

L_k — количество запросов на обработку информации на временном интервале $[t_{(\text{н})k}, t_{(\text{о})\,k}]$.

Максимально допустимое время $\tau_{(\text{доп})}$ реализации информационных процессов в СРВ определяется нормативным временем обработки информации применительно к конкретной ситуации.

С учетом изложенного можно сделать вывод о том, что вероятность $P(\tau_{(\text{ип})} \le \tau_{(\text{доп})})$ является достаточно полной характеристикой своевременной реализации информационных процессов в СРВ, что является основанием целесообразности использования ее в качестве соответствующего показателя эффективности:

$$E_{(\text{ип})} = P(\tau_{(\text{ип})} \le \tau_{(\text{доп})}).$$

Особенностью синтеза показателя защищенности информационных процессов в СРВ, обеспечиваемой механизмами защиты встраиваемого типа, является то, что они реализуются в рамках информационных процессов и процесс их реализации сопряжен с необходимостью отвлечения части временного ресурса СРВ.

С целью обоснования данного показателя представим механизмы обеспечения защиты информации совокупностью состояний $S_1 \div S_5$.

Каждое из этих состояний характеризуется соответствующей вероятностью:

$P_{(\text{к})}$ — вероятность своевременной реализации процедуры $\rho_1^{(\text{з})}$ контроля информационного процесса на предмет его подверженности угрозам информационной безопасности, представляющая собой вероятность того, что процесс защиты информации находится в состоянии S_1;

$P_{(\text{ов})}$ — вероятность своевременной реализации процедуры $\rho_2^{(\text{з})}$ обнаружения воздействий угроз информационной безопасности, представляющая собой условную вероятность того, что процесс защиты информации находится в состоянии S_2, при условии, что он уже находился в состоянии S_1, т. е. $P_{(\text{ов})} = P_{(\text{ов})}(S_2 | S_1)$;

$P_{(\text{пи})}$ — вероятность своевременной реализации процедуры $\rho_3^{(\text{з})}$ подавления источников угроз информационной безопасности, представляющая собой условную вероятность того, что процесс защиты информации находится в состоянии S_3, при условии, что он уже находился в состояниях S_1 и S_2, т. е. $P_{(\text{пи})} = P_{(\text{пи})}(S_3 | S_1 \cdot S_2)$;

$P_{(\text{ап})}$ — вероятность реализации процедуры $\rho_4^{(\text{з})}$ анализа последствий воздействий угроз информационной безопасности, представляющая собой условную вероятность того, что процесс защиты информации находится в состоянии S_4, при условии, что он уже находился в состояниях S_1, S_2 и S_3, т. е. $P_{(\text{ап})} = P_{(\text{ап})}(S_4 | S_1 \cdot S_2 \cdot S_3)$;

$P_{(\text{вц})}$ — вероятность реализации процедуры $\rho_5^{(\text{з})}$ восстановления целостности вычислительной среды, представляющая собой условную вероятность того, что процесс защиты информации находится в состоянии S_5, при условии, что он уже находился в состояниях S_1, S_2, S_3 и S_4, т. е. $P_{(\text{вц})} = P_{(\text{вц})}(S_5 | S_1 \cdot S_2 \cdot S_3 \cdot S_4)$.

Своевременность выполнения процедур $\rho_1^{(\text{з})} \div \rho_3^{(\text{з})}$ определяется условием:

$$\tau_{(\text{к})} + \tau_{(\text{ов})} + \tau_{(\text{пи})} \le \tau_{(\text{су})}, \qquad (2)$$

в котором $\tau_{(к)}$ — время, затрачиваемое на контроль информационных процессов на предмет их подверженности угрозам информационной безопасности;

$\tau_{(ов)}$ — время, затрачиваемое на обнаружение воздействий угроз;

$\tau_{(пи)}$ — время, затрачиваемое на подавление источников угроз;

$\tau_{(су)}$ — время существования угрозы.

Своевременность выполнения процедур $\rho_4^{(з)}$ и $\rho_5^{(з)}$ определяется условием:

$$\tau_{(ап)} + \tau_{(вц)} \leq \tau_{(тр)}, \qquad (3)$$

в котором $\tau_{(ап)}$ — время, затрачиваемое на анализ последствий воздействий угроз информационной безопасности;

$\tau_{(вц)}$ — время, затрачиваемое на восстановление целостности вычислительной среды СРВ;

$\tau_{(тр)}$ — требуемое (минимально допустимое) время восстановления информационных процессов в СРВ.

С учетом изложенного можно сделать вывод о том, что вероятность $\rho_{(о)}$ выполнения условия (2) является достаточно полной характеристикой своевременной реализации функций обнаружения и подавления угроз информационной безопасности СРВ, а вероятность $\rho_{(в)}$ выполнения условия (3) является достаточно полной характеристикой своевременной реализации функций восстановления информационных процессов в СРВ, подвергшихся воздействию угроз.

Соответствующий показатель:

$$E_{(ип)} = \rho_{(о)} \cdot \rho_{(в)}$$

является достаточно полной характеристикой своевременной реализации функций обеспечения защищенности информационных процессов в СРВ.

Обоснованные показатели могут быть использованы при решении широкого круга задач, связанных с исследованием различных вариантов организации информационных процессов в СРВ в условиях обеспечения их защищенности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Герасименко В. А., Малюк А. А.* Основы защиты информации: учебник для высших учебных заведений Министерства общего и профессионального образования РФ. М.: МИФИ, 1997. — 538 с.