УДК 681.322.067

А.В. Барабанов, А.С. Марков, В.Л. Цирлов, А.С. Корсунский

ИНСПЕКЦИОННЫЙ КОНТРОЛЬ ЗА СТАБИЛЬНОСТЬЮ ХАРАКТЕРИСТИК СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Барабанов Александр Владимирович, *окончил Московский государственный технический университет им. Н.Э. Баумана. Руководитель группы департамента тестирования и сертификации ЗАО «НПО «Эшелон». Имеет статьи в области анализа защищенности изделий информационных технологий от несанкционированного доступа к информации. [e-mail: mail@cnpo.ru].*

Марков Алексей Сергеевич, *кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, CISSP, SBCI. Генеральный директор ЗАО «НПО «Эшелон». Научные интересы: тестирование и сертификация программного обеспечения по требованиям безопасности информации, вопросы обеспечения надежности программного обеспечения. [e-mail: mail@npo-echelon.ru].*

Цирлов Валентин Леонидович, *кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, CISSP, AMBCI. Исполнительный директор ЗАО «НПО «Эшелон». Научные интересы: аудит защищенности и формальная верификация программного обеспечения и автоматизированных систем, управление информационной безопасностью. [e-mail: mail@npo-echelon.ru].*

Корсунский Андрей Сергеевич, *кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру Военной академии связи им. С.М. Буденного. Ведущий инженер-программист ФНПЦ ОАО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации, а также передачи информации по беспроводным каналам связи информационно-телекоммуникационных систем. [e-mail: aksspb@mail.ru].*

Аннотация

Рассмотрены вопросы проведения периодического инспекционного контроля за стабильностью характеристик сертифицированных средств защиты информации (СЗИ). Разработаны стохастические и детерминированные модели инспекционного контроля СЗИ и среды функционирования.

Ключевые слова: инспекционный контроль, периодический контроль, стохастические модели контроля, регулярный поток, поток Бернулли, сертификация, механизмы безопасности.

Alexander Vladimirovich Barabanov, *graduated from Bauman Moscow State Technical University; head of a group of the test and certification department at Echelon, JSC; author of articles in the field of analysis of information-technology product security against unauthorized access to information. e-mail: mail@cnpo.ru.*

Alexey Sergeevich Markov, *Candidate of Engineering, Associate Professor at the chair 'Information Security' of Bauman Moscow State Technical University, CISSP, SBCI; Director General of Echelon, JSC; is interested in testing and certification of software as per requirements of information security, issues of software reliability. e-mail: mail@npo-echelon.ru.*

Valentin Leonidovich Tsirlov, *Candidate of Engineering, Associate Professor at the chair 'Information Security' of Bauman Moscow State Technical University, CISSP, AMBCI; Chief Executive Officer at Echelon, JSC; is interested in security audit and formal verification of software and computer-aided systems, management of information security. e-mail: mail@npo-echelon.ru.*

Andrey Sergeevich Korsunsky, *Candidate of Engineering; graduated from the Faculty of Radio-Communications of Ulyanovsk branch of the Military Communications University; finished his post-graduate studies at the Military Communications Academy named after S. Budenny; lead programmer at Federal Research-and-Production Center 'Research-and-Production Association 'Mars'; author of articles and inventions in the field of radioelectronic protection, communications and information security as well as data transmission through wireless communications channels of infotelecommunication systems. e-mail: aksspb@mail.ru.*

Abstract

The article deals with issues of periodic inspection of stability of characteristics of certified information-security facilities. The authors have developed stochastic and deterministic models for inspections of information-security facilities and operation environment.

Key words: inspection, periodic inspection, stochastic inspection models, regular flow, Bernoulli flow, certification, security mechanisms.

Введение

Правилами обязательной сертификации средств защиты информации, устанавливаемыми в нормативных и методических документах регуляторов, предусмотрен инспекционный контроль за стабильностью характеристик СЗИ [1, 2]. Периодичность и объемы испытаний в рамках инспекционного контроля сертифицированных СЗИ определяются в нормативных и методических документах по их сертификации [1–8]. На практике после получения сертификата соответствия формируется календарный план инспекционного контроля за стабильностью характеристик сертифицированных СЗИ, согласно которому проверки проводятся через детерминированные промежутки времени.

По причине необходимости выделения дополнительных средств на испытания СЗИ после сертификации, число моментов контроля является заранее обоснованной конечной величиной. Однако в реальной жизни по ряду случайных факторов сложно организовать инспекционный контроль через строго заданные промежутки времени. Поэтому представляет интерес исследование моделей инспекционного контроля, в которых период контроля может быть как детерминированным, так и стохастическим, но при заданном числе моментов контроля.

Процедуры инспекционного контроля

В широком смысле инспекционный контроль представляет собой систематическое наблюдение за деятельностью по оценке соответствия как основы поддержания правомерности сертификата соответствия. При этом, согласно ГОСТ Р ИСО/МЭК 15408–2008, контроль касается не только СЗИ (объекта оценки), но и среды функционирования. В таком случае инспекционный контроль может включать как процедуры контроля характеристик СЗИ, так и процедуры контроля характеристик среды функционирования. Рассмотрим стохастические и детерминированные модели указанных процедур.

Модели инспекционного контроля средств защиты информации

Рассмотрим t – период жизненного цикла СЗИ с учетом проводимого инспекционного контроля за стабильностью характеристик. Поскольку период времени t во много раз превышает время контроля, положим последнее мгновенным. Тогда степень стабильности характеристик СЗИ характеризуется вероятностью $P(\hat{z} < Q) = F_{\hat{z}}(Q)$ того, что время обнаружения нарушения (уязвимости, ошибки) в межконтрольном интервале T не превосходит допустимое время Q жизненного цикла СЗИ при наличии нарушения. Фрагмент инспекционного контроля представлен на рисунке 1.

Будем считать поток нарушений (ошибок, уязвимостей) простейшим с плотностью распределения интервала между ними:

$$g_{\hat{y}} = \lambda e^{(-\lambda y)},$$

где λ – интенсивность нарушений.

Зададим стохастическую модель обнаружения нарушений. В этом случае контроль производится определенное число раз с равной вероятностью независимо друг от друга. Таким образом, образованный всеми моментами контроля ограниченный поток является потоком Бернулли с плотностью распределения интервала $\hat{T}$ между моментами контроля [9]:

$$f_{\hat{T}} = n / t\left(1 - T / t\right)^{n-1},$$

где n – число моментов контроля.

Величина задержки $\hat{z} = \hat{T} - \hat{y}$ является функцией двух случайных величин и имеет следующую функцию распределения:

$$F_{\hat{z}}^{s} = \iint_{(s)} n / t(1 - T / t)^{n-1} \lambda e^{-\lambda y}\, dTdy.$$

Определив пределы интегрирования (рис. 2), получим:

$$F_{\hat{z}}^{s} = \int_{0}^{t-z}\left(\int_{y}^{y+z} n / t(1 - T / t)^{n-1} \lambda e^{-\lambda y} dT\right)dy + \int_{t-z}^{t}\left(\int_{y}^{t} n / t(1 - T / t)^{n-1} \lambda e^{-\lambda y} dT\right)dy.$$

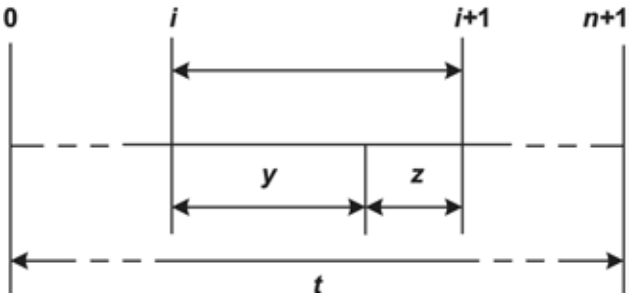

Рис. 1. Фрагмент инспекционного контроля средства защиты информации

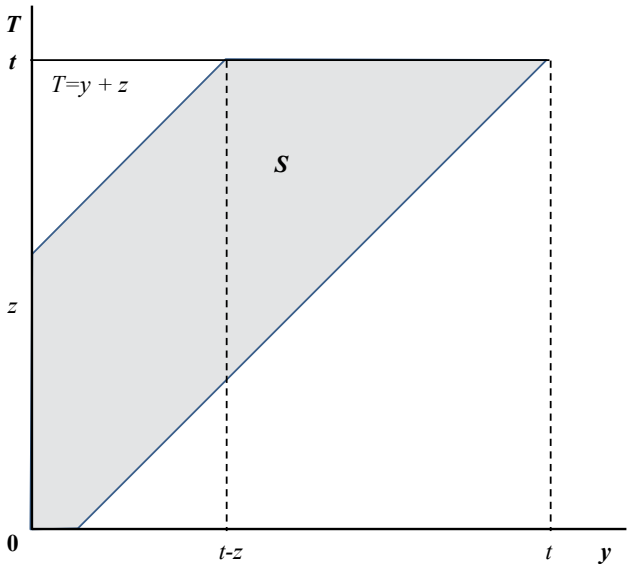

Рис. 2. Область интегрирования интервала задержки времени обнаружения нарушения

После упрощения имеем следующее выражение:

$$F_{\hat{z}}^{s} = \lambda / t^{n} \left(\int_{0}^{t-z} e^{-\lambda y} \left((t-y)^{n} - (t-z-y)^{n} \right) dy + \int_{t-z}^{t} e^{-\lambda y} \left((t-y)^{n} \right) dy \right).$$

Разложив в степенной ряд подынтегральные выражения формулы, получим приближенное значение функции распределения, которое и является основным расчетным соотношением:

$$F_{\hat{z}}^{s} = \lambda \sum_{i=0}^{n} \sum_{j=0}^{r} \sum_{l=1}^{n+j+1} (-1)^{i+j+l+1} C_{n}^{i} C_{n+j+1}^{l} \frac{\lambda^{j} t^{j+1-l_z l}}{j!(1+j+i)}, \quad (1)$$

где r – число итераций.

Для сравнения стохастической модели (1) с детерминированной рассмотрим последнюю подробнее. В детерминированной модели моменты контроля образуют регулярный поток с постоянной величиной интервала $T = t/(n+1)$ и плотностью распределения времени обнаружения нарушения:

$$g_{\hat{z}} = \lambda e^{(-\lambda(T-z))}; \; 0 < z < T.$$

Можно показать, что выражение для функции распределения в детерминированной модели имеет следующий вид:

$$F_{\hat{z}}^{d} = e^{-\lambda T} \left(e^{\lambda z} - 1 \right); \; 0 < z < T. \quad (2)$$

Сравнивая выражения (1) и (2), можно говорить о соответствии рассмотренных моделей процессу выявления нарушений стабильности характеристик СЗИ (при заданных значениях λ, Q, t и n):

$$F_{\hat{z}}^{s}(z) \leqslant F_{\hat{z}}^{d}(z).$$

Вероятность P_n обнаружения нарушений за t–период жизненного цикла СЗИ можно представить следующим образом:

$$P_n = (n+1) \cdot F_{\hat{z}},$$

где n – число моментов инспекционного контроля, $F_{\hat{z}} = max\left(F_{\hat{z}}^{s}(z), F_{\hat{z}}^{d}(z)\right)$.

Анализ рассмотренных моделей показал преимущество стохастической модели при небольшом числе моментов инспекционного контроля. Понятийно это может быть объяснено тем, что даже при малом числе случайных моментов контроля характеристик СЗИ всегда существует вероятность того, что обнаружение нарушения будет произведено сразу же при его возникновении, в то время как при использовании детерминированной модели период проверки не может быть меньше заданной величины.

Модели инспекционного контроля среды функционирования

Контроль ограничений, предъявляемых к СЗИ, в первую очередь касается проверки среды и условий функционирования и производства СЗИ. Такие проверки позволяют исключить появление нарушений (ошибок, уязвимостей), касающихся внешнего интерфейса СЗИ. В этом смысле процедуры обнаружения нарушений среды можно интерпретировать как механизм предупреждения нарушений СЗИ.

При разработке моделей контроля среды будем придерживаться подхода, приведенного в предыдущем разделе. Будем считать, что степень стабильности характеристик СЗИ определяется вероятностью $P\left(\hat{z} < Q\right) = F_{\hat{z}}(Q)$ того, что время предварительного контроля $\hat{z}$ между моментом контроля среды и возможным моментом наступления нарушения характеристик СЗИ не превосходит допустимое время Q. Зададим стохастическую модель контроля нарушений среды (рис. 3).

Можно показать, что величина времени предварительного контроля является функцией двух случайных величин $\hat{z} = \hat{y} - \hat{T}$ и имеет следующую функцию распределения:

$$F_{\hat{z}}^{s} = \iint_{(s)} n/t \left(1 - T/t\right)^{n-1} \lambda e^{-\lambda y} dT dy,$$

где n – число моментов контроля среды, λ – интенсивность нарушений характеристик СЗИ.

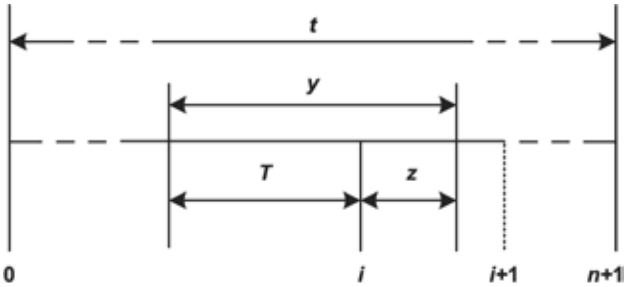

Рис. 3. Модель функционирования системы при наличии механизма предупреждения нарушений

Определив пределы интегрирования (рис. 4) и упростив выражение, получим:

$$F_{\hat{z}}^{s} = \int_{0}^{z} f_{\hat{T}}(T)\, e^{-\lambda T}\left(1-e^{-\lambda T}\right) dT + \int_{t-z}^{z} f_{\hat{T}}(T)\, e^{-\lambda T}\left(1-e^{-\lambda z}\right) dT + \int_{t-z}^{t} f_{\hat{T}}(T)\, e^{-\lambda T} dT - e^{-\lambda t}\left(\frac{z}{t}\right)^{n}.$$

Разложив в степенной ряд подынтегральные выражения, получим приближенное значение функции распределения, которое является основным расчетным соотношением:

$$F_{\hat{z}}^{s} \approx n\sum_{i=0}^{r}\left(\sum_{j=0}^{n-1} b_1 b_2\right) - e^{-\lambda t}\left(\frac{z}{t}\right)^{n}, \qquad (3)$$

где r – число итераций;

$$b_1 = (-1)^{-I+J} C_{n-1}^{i} \frac{\lambda^{j}}{\left(j!\, t^{i+1}\left(i+j+1\right)\right)};$$

$$b_2 = t^{i+j+1} - z^{i+j+1}\left(2^{j} - e^{-\lambda z}\right)\left(t-z\right)^{i+j+1} e^{-\lambda z}.$$

Сравним полученную стохастическую модель (3) с детерминированной. В детерминированной модели моменты контроля образуют регулярный поток с постоянной величиной интервала $T = t/(n+1)$ и следующей плотностью распределения времени предварительного контроля:

$$g_{\hat{z}} = \lambda e^{-\lambda(T+z)}.$$

Следовательно, выражение для функции распределения в детерминированной модели будет иметь следующий вид:

$$F_{\hat{z}}^{d} = e^{-\lambda T}\left(1-e^{-\lambda z}\right);\ 0 < z < T. \qquad (4)$$

Сравнивая выражения (3) и (4), при заданных значениях λ, Q, t и n получаем критерий, позволяющий сделать выбор той или иной модели:

$$F_{\hat{z}}^{s}(z) \lesseqgtr F_{\hat{z}}^{d}(z).$$

Вероятность предупреждения нарушений за t–период жизненного цикла СЗИ можно представить следующим образом:

$$P_n = (n+1)\cdot F_{\hat{z}},$$

где n – число моментов контроля,

$$F_{\hat{z}} = max\left(F_{\hat{z}}^{s}(z), F_{\hat{z}}^{d}(z)\right).$$

Заключение

В работе рассмотрены стохастические и детерминированные модели инспекционного контроля за стабильностью характеристик сертифицированных СЗИ, учитывающие ограничения на число моментов контроля. Представление моментов контроля в виде потока Бернулли дает возможность получить случайные временные интервалы при заданном числе этих интервалов, что позволяет учесть стохастические внешние факторы жизненного

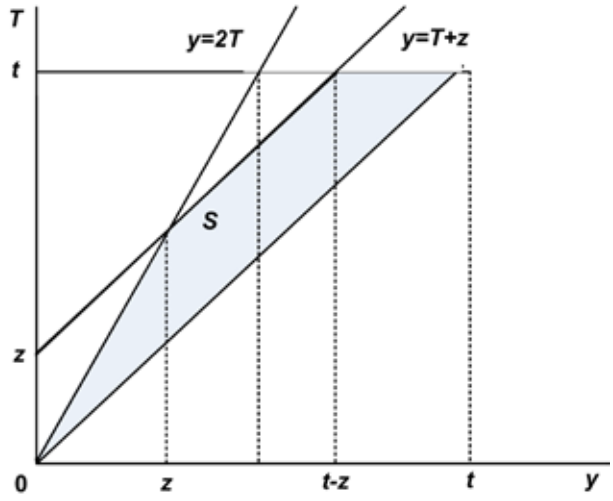

Рис. 4. Область интегрирования интервала времени предупреждения нарушения

цикла СЗИ.

Сравнительный анализ стохастических и детерминированных моделей показал эффективность первых при малом числе моментов контроля. Поэтому при управлении информационной безопасностью систем численными методами можно определить предпочтительные модели (стохастическую, детерминированную либо комбинированную), повышающие уровень доверия к СЗИ. Это дает эффект, подобный введению структурной избыточности, то есть можно говорить об особом виде избыточности – стохастическом, использование которого практически не увеличивает затрат [9]. Для удобства применения стохастических моделей можно использовать генератор случайных импульсов, позволяющий формировать случайные ограниченные потоки Бернулли [10].

Аналогичный подход был положен в основу решения задачи оценки эффективности механизма диагностики сбоев информационных массивов [11, 12]. Помимо области инспекционного контроля характеристик СЗИ изложенные результаты могут быть полезны при организации различных видов периодического контроля технических систем и систем менеджмента.

СПИСОК ЛИТЕРАТУРЫ

1. Положение о сертификации средств защиты информации по требованиям безопасности информации. – М. : Гостехкомиссия России, 1995. – 20 с.

2. Марков А.С., Цирлов В.Л. Сертификация программ: мифы и реальность // Открытые системы. СУБД. – 2011. – № 6. – С. 26–29.

3. Зубарев И.В. Сертификация как направление повышения безопасности информационных систем и программного обеспечения // Известия Таганрогского государственного радиотехнического университета. – 2003. – Т. 33, № 4. – С. 48–53.

4. Современные методы проведения сертификационных испытаний программного кода при отсутствии исходных текстов / Корсунский А.С. [и др.] // Автоматизация

процессов управления. – 2011. – № 2 (24). – С. 78–80.

5. Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. – М. : Вооружение. Политика. Конверсия, 1996. – 280 с.

6. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия Таганрогского государственного радиотехнического университета. – 2006. – Т. 62, № 7. – С. 82–87.

7. Тестирование и испытания программного обеспечения по требованиям безопасности информации / Марков А.С. [и др.] // Известия Института инженерной физики. – 2009. – № 2 (12). – С. 2–6.

8. Barabanov B., A. Markov A., A. Fadin A. Software Certification without Source Codes // Open Systems. – 2011. – №4. – pp. 38–41.

9. Марков А.С. Решение вычислительной задачи при наличии временных ограничений // Известия высших учебных заведений. Приборостроение. – 1992. – Т. 35, № 5. – С. 54–57.

10. А.с. 840856 СССР, М. Кл3, G 07 С 15/00. Генератор случайных импульсов / В.А. Керножицкий [и др.] – заявл. 06.10.78; опубл. 25.06.81, Бюлл. 23.

11. Марков А.С. К вопросу об обеспечении бесперебойной работы электронного архива // Наука и образование: электронное научно-техническое издание. – 2011. – № 7. – С. 1–8.

12. Markov A., Kernozitsky B. Economically effective data bases diagnostics method // Advances in Modeling and Analysis B: Signals, Information, Data, Patterns. 1995. Vol. 33, No. 1–3, pp. 5–12.