УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2015 Том 15 № 2 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2015 Vol. 15 No 2 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 681.324

ОПТИМИЗАЦИЯ ПЕРИОДИЧНОСТИ КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

В.А. Богатырев[a], А.В. Богатырев[a,b]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[b] Санкт-Петербургский Центр Разработок EMC, Санкт-Петербург, 199004, Российская Федерация
Адрес для переписки: Vladimir.bogatyrev@gmail.com

Информация о статье
Поступила в редакцию 05.05.14, принята к печати 05.02.15
doi:10.17586/2226-1494-2015-15-2-300-304
Язык статьи – русский
Ссылка для цитирования: Богатырев В.А., Богатырев А.В. Оптимизация периодичности контроля защищенности компьютерных систем // Научно-технический вестник информационных технологий, механики и оптики. 2015. Том 15. № 2. С. 300–304.

Аннотация. Исследованы средства контроля защищенности компьютерных систем, подверженных деструктивным воздействиям случайного и злонамеренного характера. Предложена модель оптимизации интервалов тестового контроля по обнаружению опасных состояний нарушения защищенности, вызванных деструктивными воздействиями. Оптимизация проводится с целью максимизации прибыли при обслуживании запросов в условиях неопределенности и вариантности интенсивности деструктивных воздействий с учетом штрафов при обслуживании запросов в опасных состояниях. Предложено свести векторную задачу максимизации готовности системы и минимизации вероятностей ее простоев и опасных состояний к скалярной задаче оптимизации на основе критерия максимизации прибыли от информационных услуг (обслуживания запросов), позволяющего интегрировать указанные частные критерии. Рассмотрены варианты оптимизации с определением усредненной периодичности контроля и с адаптацией этих периодов к изменениям интенсивности деструктивных воздействий. Показана эффективность адаптации периодичности контроля к изменениям активности деструктивных воздействий. Предложенные решения могут быть использованы для оптимизации интервалов тестового контроля опасных состояний нарушения защищенности, что позволяет увеличить эффективность работы системы, в том числе максимизировать ожидаемую прибыль от предоставления информационных услуг.

Ключевые слова: марковская модель, контроль, опасные состояния, деструктивные воздействия, оптимизация, интервалы тестирования.
Благодарности. Работа выполнена в рамках НИР «Методы и модели обеспечения интегрированной безопасности и устойчивости функционирования компьютерных систем».

FREQUENCY OPTIMIZATION FOR SECURITY MONITORING OF COMPUTER SYSTEMS

V.A. Bogatyrev[a], A.V. Bogatyrev[a,b]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
[b] EMC St. Petersburg Center of Excellence, Saint Petersburg, 199004, Russian Federation
Corresponding author: Vladimir.bogatyrev@gmail.com

Article info
Received 05.05.14, accepted 05.02.15
doi:10.17586/2226-1494-2015-15-2-300-304
Article in Russian
For citation: Bogatyrev V.A., Bogatyrev A.V. Frequency optimization for security monitoring of computer systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2015, vol.15, no. 2, pp. 300–304. (in Russian)

Abstract. The subject areas of the proposed research are monitoring facilities for protection of computer systems exposed to destructive attacks of accidental and malicious nature. The interval optimization model of test monitoring for the detection of hazardous states of security breach caused by destructive attacks is proposed. Optimization function is to maximize profit in case of requests servicing in conditions of uncertainty, and intensity variance of the destructive attacks including penalties when servicing of requests is in dangerous conditions. The vector task of system availability maximization and minimization of probabilities for its downtime and dangerous conditions is proposed to be reduced to the scalar optimization problem based on the criterion of profit maximization from information services (service of requests) that integrates these private criteria. Optimization variants are considered with the definition of the averaged periodic activities of monitoring and adapting of these periods to the changes in the intensity of destructive attacks. Adaptation efficiency of the monitoring frequency to changes in the activity of the destructive attacks is shown. The proposed solutions can find their application for optimization of test monitoring intervals to detect hazardous conditions of security breach that makes it possible to increase the system

effectiveness, and specifically, to maximize the expected profit from information services.
Keywords: Markov model, monitoring, hazardous conditions, destructive attacks, optimization, testing intervals.
Acknowledgements. The work is carried out within S&R engineering "Methods and Models for Integrated Security and Robustness of Computer Systems".

Введение

Эффективность предоставления информационных услуг во многом определяется надежностью, информационной и функциональной безопасностью [1–3] компьютерных систем и сетей, достигаемых при реализации комплекса программно-аппаратных средств оперативного и тестового контроля [4–6], направленных на обнаружение и минимизацию последствий деструктивных воздействий как злонамеренного, так и случайного характера [4–6].

Для компьютерных систем с целью повышения готовности к безопасному выполнению запросов и минимизации опасных состояний нарушения защищенности, существенно снижающих рентабельность предоставления информационных услуг, возникает потребность оптимизации интервалов тестирования для обнаружения нарушений защищенности в результате деструктивных воздействий.

Для систем предоставления информационных услуг, подверженных деструктивным воздействиям, оптимизация контроля на основе известных из теории надежности моделей [1, 5, 6] контроля не позволяет учесть условия функционирования защищенных информационных систем, так как интенсивность злонамеренных воздействий (в отличие от отказов), как правило, характеризуется неопределенностью и частой изменяемостью во времени. Эта особенность обусловливает потребность модификации марковской модели контроля и постановки задачи оптимизации интервалов тестирования с целью учета неопределенности и изменяемости интенсивностей деструктивных воздействий. При решении поставленной задачи предлагается свести векторную задачу максимизации готовности системы и минимизации вероятностей ее простоев и опасных состояний к скалярной задаче оптимизации на основе критерия максимизации прибыли от информационных услуг (обслуживания запросов), позволяющего интегрировать указанные частные критерии. Разрабатываемая модель должна позволить оценить эффективность контроля с адаптацией периодичности тестирования к изменениям интенсивности вредоносных воздействий с учетом разрешения технического противоречия, связанного с достижением максимума готовности системы к безопасному предоставлению информационных услуг, минимума ее простоев, связанных с тестированием и восстановлением защищенности, а также минимума вероятности опасных состояний необнаруженных нарушений защищенности.

Модель контроля защищенности

При построении марковской модели исследуемой системы выделим состояния: готовности системы к безопасному выполнению запросов (0); тестирования в отсутствии нарушений защищенности (1); восстановления безопасности (2); необнаруженных нарушений защищенности (3); тестирования при наличии нарушений (4). Состояние необнаруженных нарушений защищенности является опасным. Граф состояний и переходов системы в предположении идеальности тестового контроля по обнаружению всех нарушений защиты приведен на рис. 1. По этому графу составляется система уравнений Колмогорова–Чепмена [7–9], позволяющая с использованием средств компьютерной математики вычислить вероятности всех состояний системы:

$$P_0 = \lambda_1\mu_0\mu_1 W,\ P_1 = \lambda_1^2\mu_0 W,\ P_2 = \mu_1\lambda_0\lambda_1 W,\ P_3 = \lambda_0\mu_0\mu_1(1-g)W,\ P_4 = \lambda_0\lambda_1\mu_0(1-g)W,$$

где $W = \left(\lambda_1^2\mu_0 + \mu_1\lambda_0\lambda_1 + \mu_0\lambda_0\lambda_1 + \lambda_1\mu_0\mu_1 + \lambda_0\mu_0\mu_1 - g\lambda_0\mu_0\left(\lambda_1 + \mu_1\right)\right)^{-1}$.

При этом λ_0 – интенсивность деструктивных воздействий; λ_1 – интенсивность инициализация тестового контроля; g – доля обнаруживаемых оперативным контролем нарушений защищенности; μ_1 – интенсивность тестирования (величина, обратная среднему времени тестирования), μ_0 – интенсивность восстановления безопасного состояния (величина, обратная среднему времени восстановления защиты).

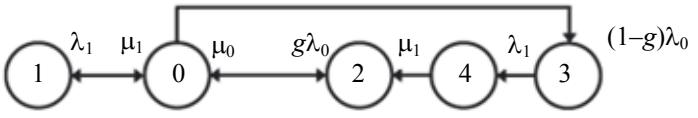

Рис. 1. Граф состояний и переходов системы

Оптимизация интервалов контроля защищенности

Модели контроля защищенности систем от злонамеренных деструктивных воздействий, в отличие от известных в теории надежности моделей контроля отказов [5, 6], должны учитывать неопределенность интенсивностей злонамеренных воздействий и их изменений во времени. При оптимизации интервалов тестирования будем предполагать заданными вектора вариантов возможных интенсивностей деструктивных воздействий **q** и вероятностей этих вариантов **r**.

Оптимизация интервалов тестирования связана с техническим противоречием между достижением максимума готовности системы и минимума вероятности ее опасных состояний. Формально решение этой задачи векторной оптимизации возможно по аддитивному или мультипликативному скалярному критерию, однако такое решение сопряжено с субъективизмом назначения весов приоритета частных критериев.

Избежать субъективности векторной оптимизации позволяет формирование объективного критерия, имеющего некоторый физический смысл и интегрирующего частные критерии [10]. В качестве такого критерия предлагается критерий – прибыль от обслуживания запросов. Будем считать, что каждый запрос, поступающий в состоянии готовности системы к его безопасному выполнению, обеспечивает прибыль s_0, а в состоянии простоя – прибыль s_1 ($s_1<s_0$, что обусловлено дополнительными задержками по завершению тестирования и (или) восстановления системы после обнаружения ее нарушений). Запрос, поступающий в опасном состоянии необнаруженных нарушений защищенности, приводит к убыткам (штрафу) s_3. Таким образом, математическое ожидание прибыли от обслуживания запроса вычисляется как

$$S = s_0 P_0 - s_3 P_3 + s_1 (1 - P_0 - P_3).$$

При неопределенности потока деструктивных воздействий рассмотрим варианты В1–В3 оптимизации интервалов тестирования, обеспечивающих максимум прибыли при обслуживании запросов.

При варианте В1 определяется значение интервала тестирования $1/\lambda_1$, обеспечивающее максимум прибыли при обслуживании запросов, по критерию

$$\max_{\lambda_1} \left(\frac{\lambda_1 \mu_0 \mu_1 s_0 - s_3 \lambda_0 \mu_0 \mu_1 (1-g) + s_1 (1 - \lambda_1 \mu_0 \mu_1 - \lambda_0 \mu_0 \mu_1 (1-g))}{\left({\lambda_1}^2 \mu_0 + \mu_1 \lambda_0 \lambda_1 + \mu_0 \lambda_0 \lambda_1 + \lambda_1 \mu_0 \mu_1 + \lambda_0 \mu_0 \mu_1 - g \lambda_0 \mu_0 (\lambda_1 + \mu_1) \right)} \right)$$

при средней интенсивности воздействий $\lambda_0 = \sum_{i=0}^{n-1} q_i r_i$.

При варианте В2 с учетом всех возможных интенсивностей воздействий q_i ($i = 0,1,\ldots,n-1$) определяется оптимальный, усредненный по всем интенсивностям воздействий, интервал тестирования $1/\lambda_1$, обеспечивающий максимум прибыли обслуживания запросов, по критерию

$$\max_{\lambda_1} \sum_{i=0}^{n-1} r_i \left(\frac{\lambda_1 \mu_0 \mu_1 s_0 - s_3 q_i \mu_0 \mu_1 (1-g) + s_1 (1 - \lambda_1 \mu_0 \mu_1 - q_i \mu_0 \mu_1 (1-g))}{\left({\lambda_1}^2 \mu_0 + \mu_1 q_i \lambda_1 + \mu_0 q_i \lambda_1 + \lambda_1 \mu_0 \mu_1 + q_i \mu_0 \mu_1 - g q_i \mu_0 (\lambda_1 + \mu_1) \right)} \right),$$

где q_i – i-й вариант возможной интенсивности деструктивных воздействий, вероятность которой r_i.

При варианте В3 для возможных интенсивностей деструктивных воздействий, задаваемых вектором **q**, определяется вектор оптимальных интенсивностей инициализации тестирования **a**, обеспечивающих максимум прибыли обслуживания запросов, по критерию

$$\max_{\mathbf{a}} \sum_{i=0}^{n-1} r_i \left(\frac{a_i \mu_0 \mu_1 s_0 - s_3 q_i \mu_0 \mu_1 (1-g) + s_1 (1 - a_i \mu_0 \mu_1 - q_i \mu_0 \mu_1 (1-g))}{{a_i}^2 \mu_0 + \mu_1 q_i a_i + \mu_0 q_i a_i + a_i \mu_0 \mu_1 + q_i \mu_0 \mu_1 - g q_i \mu_0 (a_i + \mu_1)} \right).$$

Адаптация интервалов тестирования в процессе функционирования требует периодических измерений (мониторинга) интенсивностей деструктивных воздействий с определением градаций интенсивности q_i и соответствующих интервалов тестирования (предварительно установленных при оптимизации или рассчитываемых в реальном времени). Следует заметить, что адаптация интервалов тестирования может вызвать замедление вычислительного процесса, а поэтому требует сравнения выигрыша и затрат на ее реализацию.

Пример оптимизации

Приведем пример оптимизации интервалов тестирования системы по критерию максимизации прибыли. Будем считать, что заданы $\mu_1 = 1$ ч$^{-1}$, $\mu_0 = 0{,}1$ ч$^{-1}$, $g = 0{,}6$, $s_0 = 1$ у.е., $s_1 = 0{,}1$ у.е., $s_2 = 100$ у.е., варианты интенсивностей деструктивных воздействий и их вероятности, представленные векторами **q** = (0,001; 0,002; 0,003; 0,004; 0,005; 0,006) и **r** = (0,1; 0,15; 0,3; 0,2; 0,15; 0,1). Для вариантов В1, В2 оптимальным интервалам тестирования, обеспечивающим максимум прибыли S при обслуживании каждого запроса, соответствуют $\lambda_1 = 0{,}5824$ ч$^{-1}$ и $\lambda_1 = 0{,}5802$ ч$^{-1}$. Для варианта В3 вектор оптимальных интенсивностей инициализации тестирования **a**, обеспечивающий максимум прибыли S при обслуживании каждого запроса, равен **a** = (0,020; 0,028; 0,035; 0,040; 0,045; 0,049).

Результаты расчета математического ожидания максимально возможной прибыли от выполнения запроса с адаптацией периодичности контроля к изменениям интенсивности деструктивных воздействий и и без нее представлены на рис. 2. Кривая 1 соответствует варианту В3 адаптивного изменения периодов контроля в зависимости от наблюдаемой интенсивности деструктивных воздействий. Кривая 2 соответствует вариантам В1, В2, при которых задается постоянный период тестирования, независимо от реальной интенсивности деструктивных воздействий. Кривая 3 отражает разницу прибыли от обслуживания

запросов с адаптацией периода контроля к изменениям интенсивности деструктивных воздействий и без нее. Представленные графики показывают эффективность адаптации периодов тестирования защищенности к изменениям интенсивности деструктивных воздействий.

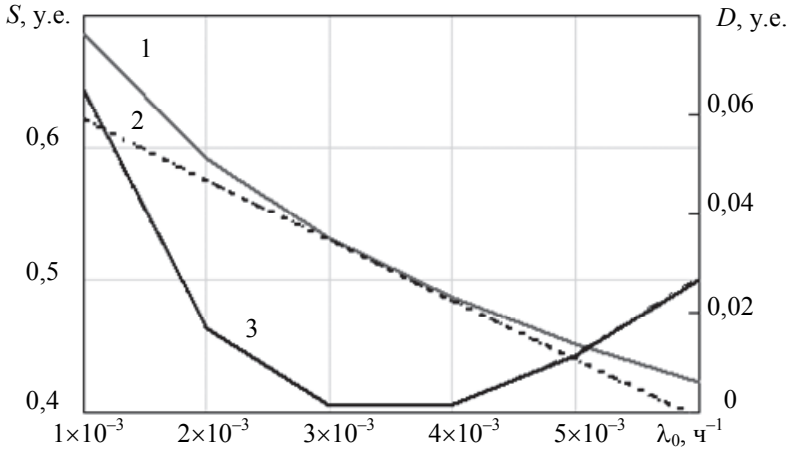

Рис. 2. Зависимость максимальной прибыли обслуживания запросов от интенсивности деструктивных воздействий: 1 – адаптивное изменение периодов контроля; 2 – постоянный период контроля; 3 – увеличение прибыли от адаптивного изменения периодов контроля, *D* – разница максимальной прибыли обслуживания запросов при адаптивном и постоянном задании периодов контроля

Предложенные варианты оптимизации тестового контроля могут найти применение при системотехническом проектировании компьютерных систем и сетей критического применения, работающих в условиях дестабилизирующих воздействий, в том числе злонамеренного характера [11–21].

Заключение

Предложена марковская модель защищенных информационных систем, функционирующих в условиях деструктивных злонамеренных и случайных воздействий, и решена задача оптимизации интервалов инициализации тестового контроля по критерию максимизации прибыли от предоставления информационных услуг с учетом неопределенности и изменяемости интенсивности деструктивных воздействий.

Рассмотрены варианты задачи оптимизации интервалов тестирования без их адаптации и с адаптацией к изменениям реальной интенсивности деструктивных воздействий.

Показана эффективность адаптивного задания периодов тестирования с целью максимизации прибыли при предоставлении информационных услуг в зависимости от измеряемой интенсивности деструктивных воздействий. При интенсивности деструктивных воздействий 0,001 $ч^{-1}$ адаптивное тестирование по сравнению с неадаптивным назначением периодов тестирования позволяет увеличить среднюю прибыль от обслуживания одного запроса примерно с 0,62 до 0,69 у.е.

Литература

1. Черкесов Г.Н. Надежность аппаратно-программных комплексов. СПб.: Питер, 2005. 479 с.
2. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Оценка вероятности эрланговского старения информации // Информационно-управляющие системы. 2013. № 6 (67). С. 25–28.
3. Богатырев В.А. К повышению надежности вычислительных систем на основе динамического распределения функций // Изв. вузов. Приборостроение. 1981. Т. 23. № 8. С. 62–65.
4. Щеглов К.А., Щеглов А.Ю. Система защиты от запуска вредоносных программ // Вестник компьютерных и информационных технологий. 2013. № 5 (107). С. 38–43.
5. Перегуда А.И. Тимашов Д.А. Вероятностный анализ показателей надежности подсистем СУЗ с учетом периодического контроля исправности // Изв. вузов. Ядерная энергетика. 2009. № 4. С. 45–53.
6. Сугак Е.В., Кучкин А.Г., Бельская Е.Н. Надежность технических систем и техногенный риск. Ч. 2. Красноярск: СибГАУ, 2013. 436 с.
7. Немолочнов О.Ф., Зыков А.Г., Осовецкий Л.Г., Поляков В.И. Методы тестирования вычислительных процессов // Научно-технический вестник СПбГУ ИТМО. 2007. № 11 (45). С. 121–125.
8. Алиев Т.И. Основы моделирования дискретных систем: Учебное пособие. СПб.: СПбГУ ИТМО. 2009. 363 с.
9. Алиев Т.И., Муравьева-Витковская Л.А. Приоритетные стратегии управления трафиком в мультисервисных компьютерных сетях // Изв. вузов. Приборостроение. 2011. Т. 54. № 6. С. 44–48.

10. Богатырев В.А., Богатырев С.В. Критерии оптимальности многоустойчивых отказоустойчивых компьютерных систем // Научно-технический вестник СПбГУ ИТМО. 2009. № 5 (63). С. 92–97.
11. Богатырев В.А., Богатырев А.В. Функциональная надежность систем реального времени // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4 (86). С. 150–151.
12. Богатырев В.А. Отказоустойчивость и сохранение эффективности функционирования многомагистральных распределенных вычислительных систем // Информационные технологии. 1999. № 9. С. 44–48.
13. Богатырев В.А. К оценке эффективности динамического распределения запросов в отказоустойчивых управляющих вычислительных системах // Приборы и системы. Управление, контроль, диагностика. 2002. № 9. С. 10–12.
14. Богатырев В.А., Богатырев С.В., Богатырев А.В. Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения // Информационные технологии. 2013. № 2. С. 27–32.
15. Богатырев В.А., Мультипроцессорные системы с динамическим перераспределением запросов через общую магистраль // Изв. вузов. Приборостроение. 1985. № 3. С. 33–38.
16. Bogatyrev V.A. Fault tolerance of clusters configurations with direct connection of storage devices // Automatic Control and Computer Sciences. 2011. V. 45. N 6. P. 330–337. doi: 10.3103/S0146411611060046
17. Bogatyrev V.A., Bogatyrev S.V., Golubev I.Yu. Optimization and the process of task distribution between computer system clusters // Automatic Control and Computer Sciences. 2012. V. 84. N 3. P. 103–111. doi: 10.3103/S0146411612030029
18. Galinina O., Andreev S., Koucheryavy Y., Turlikov A.B. Stabilizing multi-channel slotted aloha for machine-type communications // Proc. IEEE International Symposium on Information Theory (ISIT 2013). Istanbul, Turkey, 2013. Art. 6620600. P. 2119–2123. doi: 10.1109/ISIT.2013.6620600
19. Andreev S., Saffer Z., Turlikov A. Delay analysis of wireless broadband networks with non real-time traffic // Lecture Notes in Computer Science. 2011. V. 6886 LNCS. P. 206–217. doi: 10.1007/978-3-642-23795-9_18
20. Turlikov A.M., Foss S.G. On ergodic algorithms in random multiple access systems with "success-failure" feedback // Problems of Information Transmission. 2010. V. 46. N 2. P. 184–200. doi: 10.1134/S0032946010020067
21. Гатчин Ю.А., Жаринов И.О., Коробейников А.Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2 (78). С. 92–95.

Богатырев Владимир Анатольевич – доктор технических наук, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Vladimir.bogatyrev@gmail.com

Богатырев Анатолий Владимирович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; инженер-программист, Санкт-Петербургский Центр Разработок EMC, Санкт-Петербург, 199004, Российская Федерация, gangleon@gmail.com

Vladimir A. Bogatyrev – D.Sc., Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Vladimir.bogatyrev@gmail.com

Anatoly V. Bogatyrev – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation; software engineer, EMC St. Petersburg Center of Excellence, Saint Petersburg, 199004, Russian Federation, gangleon@gmail.com