УДК 621.377

В.Г. Ерышов, А.С. Корсунский, С.А. Смолин

СЕРТИФИКАЦИЯ СИСТЕМ, КОМПЛЕКСОВ, СРЕДСТВ СВЯЗИ, ЗАЩИТЫ ИНФОРМАЦИИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Ерышов Вадим Георгиевич, *кандидат технических наук, окончил Военную академию связи им. С.М. Буденного, докторантуру (там же). Доцент кафедры «Радиоэлектронная защита, безопасность связи и информации» Военной академии связи. Имеет учебные пособия, статьи и изобретения в области обеспечения электромагнитной совместимости радиоэлектронных средств военного назначения, контроля безопасности связи и информации, а также контроля защищенности информации от ее утечки по техническим каналам. [e-mail: eryshov@mail.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. [e-mail: aksspb@mail.ru].*

Смолин Сергей Анатольевич, *окончил механико-математический факультет Ульяновского государственного университета. Начальник научно-исследовательской лаборатории ФНПЦ ОАО «НПО «Марс». Имеет статьи по сертификации в области защиты информации. [e-mail: mars@mv.ru].*

Аннотация

В статье исследуется процесс сертификации по требованиям безопасности информации для выявления вероятностно-временных зависимостей событий и состояний данного процесса. Получены зависимости, которые могут использоваться для оценки эффективности функционирования существующих систем сертификации и разработки предложений по их совершенствованию.

Ключевые слова: сертификация, Марковские случайные процессы, защита информации, модель процесса сертификации.

Vadim Georgievich Eryshov*, Candidate of Engineering, graduated from and finished his doctoral studies at the Military Communications Academy named after S. Budenny; Associate Professor of the Chair 'Radio-Electronics Protection, Security of Communications and Information' at the Military Communications Academy; author of textbooks, articles and inventions in the field of electromagnetic compatibility of military-purpose radio-electronics facilities, monitoring of communications and information security as well as monitoring of information security against its leakage through technical channels. e-mail: eryshov@mail.ru.*

Andrey Sergeevich Korsunky*, Candidate of Engineering, graduated from the Faculty of Radio-Communications at Ulyanovsk branch of the Military Communications University, finished his post-graduate studies at the Military Communications Academy named after S. Budenny; lead programmer of FRPC OJSC 'RPA 'Mars'; author of articles and inventions in the field of radio-electronics protection, communications and information security. e-mail: aksspb@mail.ru.*

Sergey Anatolyevich Smolin*, graduated from the Faculty of Mechanics and Mathematics at Ulyanovsk State University; head of a research laboratory at FRPC OJSC 'RPA 'Mars'; author of articles in certification in the field of information security. e-mail: mars@mv.ru.*

Abstract

The article researches a certification process as per requirements of information security in order to detect probability and time dependences of events and states of the process. It reveals the got dependences which can be used for the estimation of effectiveness of the operation of existing systems in certification, and development of improvement suggestions.

Key words: certification, Markovian processes, information security, certification-process model.

Введение

Одной из актуальных задач при создании современных систем, комплексов и средств связи, а также средств защиты информации (СЗИ) и программного обеспечения (ПО), разрешенных к применению в силовых структурах, министерствах и ведомствах РФ, является разработка модели процесса сертификации систем, комплексов и средств связи, СЗИ и ПО, не противоречащей руководящим и нормативно-правовым документам [1–3].

Модель процесса сертификации систем, комплексов и средств связи, СЗИ и ПО

Под сертификацией систем, комплексов и средств связи, СЗИ и ПО по требованиям безопасности информации (далее сертификация) понимается деятельность по подтверждению их соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Федеральной службой по техническому и экспертному контролю (ФСТЭК) при Президенте Российской Федерации.

Деятельность системы сертификации организует ФСТЭК, Федеральная служба безопасности (ФСБ), Служба внешней разведки (СВР), Федеральная служба охраны (ФСО), Министерство обороны (МО) РФ в пределах своей компетенции, определенной законодательными и иными нормативными актами РФ.

Целями функционирования системы сертификации являются:

- обеспечение реализации требований государственной системы защиты информации;
- создание условий для качественного и эффективного обеспечения потребителей сертифицированными системами, комплексами и средствами связи, СЗИ и ПО;
- обеспечение национальной безопасности в сфере информатизации;
- содействие формированию рынка защищенных информационных технологий и средств их обеспечения;
- формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современных требований по защите информации;
- поддержка проектов и программ информатизации.

Обязательной сертификации подлежат системы, комплексы и средства связи, СЗИ и ПО, в том числе иностранного производства, предназначенные для использования в силовых министерствах, органах государственной власти, а также защиты информации, составляющей государственную тайну, и другой информации с ограниченным доступом.

Основными схемами сертификации систем, комплексов и средств связи, СЗИ и ПО являются:

- для единичных образцов – проведение испытаний на соответствие требованиям по безопасности информации;
- для серийного производства систем – проведение типовых испытаний их образцов на соответствие требованиям по безопасности информации и последующий инспекционный контроль за стабильностью характеристик сертифицированной продукции, обеспечивающих (определяющих) выполнение этих требований.

На сегодняшний день организационную структуру системы сертификации образуют:

- ФСТЭК, ФСБ, СВР, ФСО, МО РФ;
- центральный орган системы сертификации;
- органы по сертификации средств защиты информации силовых структур (ФСТЭК РФ, ФСБ, СВР, ФСО, МО);
- испытательные центры (лаборатории);
- заявители (разработчики, изготовители, поставщики, потребители).

В настоящее время сертификация систем и ПО осуществляется различными ведомствами и аккредитованными органами по сертификации по своим ведомственным нормативно-правовым и руководящим документам. Испытания же проводятся аккредитованными соответствующими ведомствами испытательными центрами (лабораториями) на их материально-технической базе, что зачастую приводит к отсутствию единой согласованной государственной политики в области сертификации данных систем по требованиям безопасности информации в целом.

В связи с этим актуальной является проблема исследования процесса сертификации для выявления вероятностно-временных зависимостей событий и состояний данного процесса и разработки предложений по модернизации и совершенствованию системы сертификации в целом.

Для решения проблемы создания единой системы сертификации с единой нормативно-правовой базой необходима ее проработка, в том числе и в теоретическом плане. В частности, для таких исследований применим аппарат теории Марковских случайных процессов.

Процесс сертификации можно представить ориентированным графом состояний и описать в терминах теории Марковских случайных процессов с дискретными состояниями и непрерывным временем. Под таким процессом будем понимать процесс, у которого в любой момент времени t множество его состояний S – счетно или конечно, а переходы из одного состояния в другое происходят в любой момент времени t наблюдаемого периода [4].

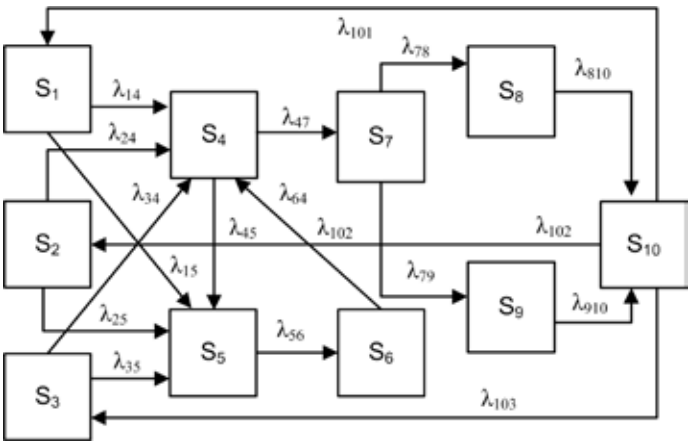

Рис. 1. Ориентированный граф состояний процесса сертификации средств связи, СЗИ и ПО

Будем полагать, что переходы из одного состояния в другое происходят под воздействием пуассоновских потоков событий [4, 5].

Ориентированный граф состояний процесса сертификации, описанного в терминах Марковских процессов с дискретными состояниями и непрерывным временем, представлен на рисунке 1.

Описание состояний данного процесса, а также входящих и выходящих потоков событий представлены в таблице.

Составим для графа, представленного на рисунке 1, систему обыкновенных дифференциальных уравнений Колмогорова [4]. Исходные данные для решения этой системы получены авторами из статистических данных от ряда лабораторий и центров сертификации за определенный отчетный период.

Решение системы обыкновенных дифференциальных уравнений Колмогорова было получено с помощью пакета математического программирования «MathCad». В результате проведенного моделирования были получены следующие вероятностные и временные зависимости состояний процесса сертификации средств связи, СЗИ и ПО от времени, представленные на рисунке 2.

Таблица

Описание состояний процесса сертификации систем, комплексов и средств связи, СЗИ и ПО

№ п/п	Наименование состояния	$\lambda_{вых}$	$\lambda_{вх}$
S_1	Поступление заявки на проведение сертификации систем, комплексов и средств связи	λ_{14}, λ_{15}	λ_{101}
S_2	Поступление заявки на проведение сертификации средств защиты информации	λ_{24}, λ_{25}	λ_{102}
S_3	Поступление заявки на проведение сертификации ПО	λ_{34}, λ_{35}	λ_{103}
S_4	Существует свободная лаборатория (отдел) сертификации	λ_{45}, λ_{47}	λ_{14}, λ_{24}, λ_{34}, λ_{64}
S_5	Не существует свободной лаборатории (отдела) сертификации, отказ в сертификации	λ_{56}	λ_{15}, λ_{25}, λ_{35}, λ_{45}
S_6	Ожидание освобождения лаборатории (отдела) сертификации	λ_{64}	λ_{56}
S_7	Сертификация	λ_{78}, λ_{79}	λ_{47}
S_8	Правильное принятие решения о классе защищенности сертифицируемого объекта	λ_{810}	λ_{78}
S_9	Ошибочное принятие решения о классе защищенности сертифицируемого объекта	λ_{910}	λ_{79}
S_{10}	Окончание сертификации, документирование ее результатов, выдача сертификата	λ_{101}, λ_{102}, λ_{103}	λ_{810}, λ_{910}

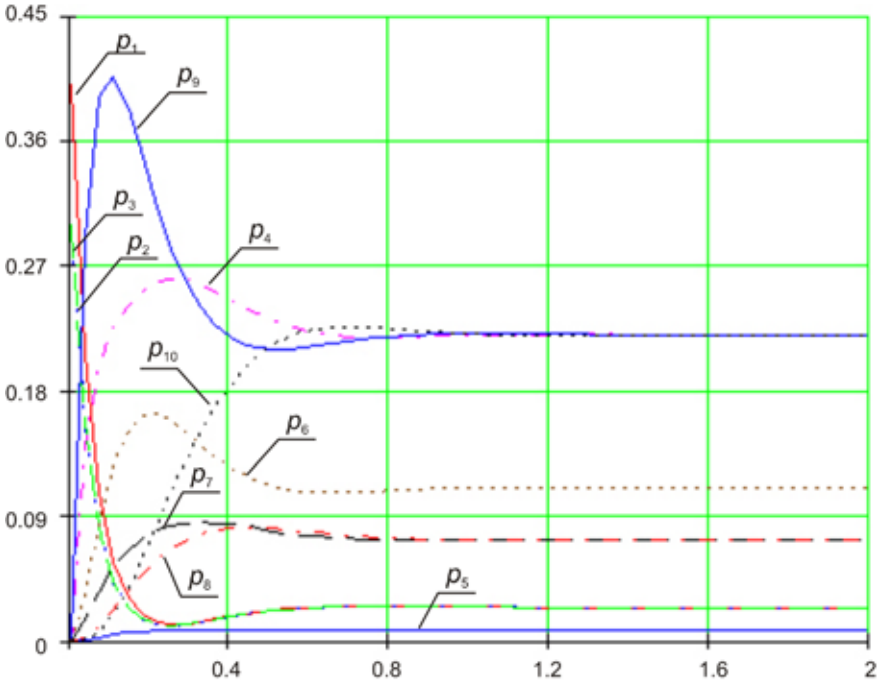

Рис. 2. Зависимости вероятностей состояний процесса сертификации от времени

$$
\begin{cases}
\dfrac{dp_1(t)}{dt} = p_{10}(t)\lambda_{101} - p_1(t)\{\lambda_{14}+\lambda_{15}\},\\
\dfrac{dp_2(t)}{dt} = p_{10}(t)\lambda_{102} - p_2(t)\{\lambda_{24}+\lambda_{25}\},\\
\dfrac{dp_3(t)}{dt} = p_{10}(t)\lambda_{103} - p_3(t)\{\lambda_{34}+\lambda_{35}\},\\
\dfrac{dp_4(t)}{dt} = p_1(t)\lambda_{14} + p_2(t)\lambda_{24} + p_3(t)\lambda_{34} +\\
\qquad + p_6(t)\lambda_{64} - p_4(t)\{\lambda_{45}+\lambda_{47}\},\\
\dfrac{dp_5(t)}{dt} = p_1(t)\lambda_{15} + p_2(t)\lambda_{25} + p_3(t)\lambda_{35} +\\
\qquad + p_4(t)\lambda_{45} - p_5(t)\lambda_{56},\\
\dfrac{dp_6(t)}{dt} = p_5(t)\lambda_{56} - p_6(t)\,\lambda_{64},\\
\dfrac{dp_7(t)}{dt} = p_4(t)\lambda_{47} - p_7(t)\{\lambda_{78}+\lambda_{79}\},\\
\dfrac{dp_8(t)}{dt} = p_7(t)\lambda_{78} - p_8(t)\lambda_{810},\\
\dfrac{dp_9(t)}{dt} = p_7(t)\lambda_{79} - p_9(t)\,\lambda_{910},\\
\dfrac{dp_{10}(t)}{dt} = p_8(t)\lambda_{810} + p_9(t)\,\lambda_{910} -\\
\qquad - p_{10}(t)\{\lambda_{101}+\lambda_{102}+\lambda_{103}\},
\end{cases}
\qquad (1)
$$

$$\sum_{i}^{10} p_i(t) = 1.$$

Анализ полученных результатов (рис. 2) показывает, каким образом изменяются состояния процесса сертификации средств связи, СЗИ и ПО на временной оси.

Так, например, в начальный момент модельного времени ($t = 0.1$) система сертификации находится с максимальными вероятностями p_1, p_2, p_3 в состояниях поступления заявок на проведение сертификационных испытаний систем, комплексов и средств связи, СЗИ и ПО. Далее при $t = 0.2$ модельной единицы система сертификации находится с максимальной вероятностью $p_4 = 0.25$ в состоянии существования свободных лабораторий (отделов) сертификации. Затем при $t = 0.4$ модельной единицы в системе сертификации уменьшаются свободные лаборатории (отделы) сертификации.

Начиная с момента времени наблюдаемого периода $t = 1$ модельной единицы, процесс сертификации становится стационарным процессом с финальными вероятностями $P_i(t) = P_i = const$ и с максимальной вероятностью $p_{10} = 0.23$, т. е. система сертификации переходит в состояние окончания сертификации, документирования ее результатов и выдачи сертификата соответствия. При этом вероятность правильного принятия решения о классе защищенности сертифицируемого объекта p_8 в три раза больше вероятности ошибочного принятия решения о классе защищенности сертифицируемого объекта p_9.

Итак, в статье предложен один из возможных подходов для исследования (анализа) обобщенного процесса сертификации в существующей системе сертификации любого ведомства (ФСТЭК, ФСБ, СВР, ФСО, МО РФ) или в целом единой системы сертификации с целью выявления вероятностно-временных зависимостей событий и состояний исследуемого процесса и разработки предложений по модернизации, совершенствованию и созданию эффективной системы сертификации, например, по обоснованию:

- необходимого количества лабораторий различного типа в системе сертификации с целью сокращения или устранения возможных очередей;
- возможных максимальных объемов заявок на сертификацию;
- потенциальных возможностей лабораторий по обслуживанию поступающих заявок (где можно задать временные рамки и обосновать структуру лабораторий при определенной степени детализации процесса).

Для этого разработана обобщенная, не претендующая на полноту по учету всех возможных состояний (по степени детализации), математическая модель процесса сертификации систем, комплексов и средств связи, СЗИ и ПО, описанная в терминах теории случайных Марковских процессов при определенных ограничениях и допущениях:

- процесс сертификации – случайный процесс с дискретными состояниями, т. е. количество его состояний счетно или конечно, время перехода из одного состояние в другое – непрерывно, а не дискретно;
- поток поступающих в лаборатории обслуженных заявок (сертифицированных средств, систем и ПО) и заявок на осуществление сертификации – пуассоновский;
- модель дает возможность получать вероятностные и временные зависимости, описывающие состояния исследуемого процесса сертификации при варьируемых параметрах (исходных данных) – входящих и выходящих потоках событий исследуемого процесса:
- наличие поступления заявки на проведение сертификации систем, комплексов и средств связи в лаборатории;
- существование (отсутствие) свободных лабораторий (отделов) в системе сертификации;
- ожидание освобождения лабораторий (отделов) системы сертификации;
- ожидание самого процесса сертификации;
- правильное (неправильное) принятие решения о классе защищенности сертифицируемого объекта.

Заключение

Таким образом, разработанная модель процесса сертификации систем, комплексов и средств связи, СЗИ и ПО, описанная в терминах теории случайных Марковских процессов, обладает теоретической и практической новизной и позволяет получать вероятностные и временные зависимости, описывающие состояния исследуемого процесса

при варьируемых исходных данных входящих и выходящих потоков событий.

Определенные в разработанной модели и полученные в результате моделирования зависимости являются основой для оценки эффективности функционирования существующих систем сертификации и разработки предложений по их совершенствованию, а также синтезу новых систем сертификации.

СПИСОК ЛИТЕРАТУРЫ

1. Положение о сертификации средств защиты информации по требованиям безопасности информации : утв. приказом председателя ГТК России от 27 октября 1995 г. № 199.

2. Положение о сертификации средств защиты информации» (с изм. от 21.04.2010 № 266) : утв. Постановлением Правительства РФ от 26.06.1995 № 608.

3. Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации : утв. приказом Председателя ГТК России от 25 ноября 1994 г.

4. Вентцель Е. С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. – М. Наука, 1991. – 384 с.

5. Вентцель Е. С. Исследование операций: задачи, принципы, методология.– 2-е изд., стер. – М. : Наука, 1988. – 208 с.