УДК 621.377

Ю.И. Стародубцев, В.Г. Ерышов, А.С. Корсунский

МОДЕЛЬ ПРОЦЕССА МОНИТОРИНГА БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Стародубцев Юрий Иванович, *доктор военных наук, профессор, окончил Кемеровское высшее военное командное училище связи, Военную академию связи им. С.М. Буденного. Заслуженный деятель науки РФ, академик Российской Академии военных наук, Академии безопасности и правопорядка, Российской Академии естественных наук, Арктической академии, почетный работник высшего профессионального образования. Начальник кафедры «Радиоэлектронная защита, безопасность связи и информации» Военной академии связи им. С.М. Буденного. Имеет монографии, учебные пособия, статьи и изобретения в области защиты информационного ресурса систем военной связи и АСУ в условиях информационной войны. [e-mail: vas@mail.ru].*

Ерышов Вадим Георгиевич, *кандидат технических наук, окончил Военную академию связи им. С.М. Буденного, докторантуру Военной академии связи. 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].*

Аннотация

В статье исследуется такой аспект информационного противоборства, как мониторинг безопасности информации в информационно-телекоммуникационных системах (ИТКС). Рассмотрена модель мониторинга безопасности информации в информационно-телекоммуникационных системах на основе аппарата теории Марковских случайных процессов.

Ключевые слова: мониторинг безопасности информации, информационно-телекоммуникационная система, Марковские случайные процессы.

Yury Ivanovich Starodubtsev, *Doctor of Military Sciences, Professor, graduated from the Kemerovo Command Communications Academy, the Military Communications Academy named after S. Budenny; Honoured Scientist of the Russian Federation, Academician of the Russian Academy of Military Sciences, Academy of Security and Legal Order, the Russian Academy of Natural Sciences, Academy Arctic of Sciences; honorary worker in higher vocational education; holds the Chair 'Radio-Electronics Protection, Security of Communications and Information' at the Military Communications Academy named after S. Budenny; author of monographs, text-books, articles and inventions in the field of protection of information resources of military-communications systems and C2 systems under information-war conditions. e-mail: vas@mail.ru.*

Vadim Georgievich Eryshov, *Candidate of Engineering, graduated from the Military Communications Academy named after S. Budenny, finished his doctoral studies at the Military Communications Academy; Associate Professor of the Chair 'Radio-Electronics Protection, Security of Communications and Information' at the Military Communications Academy; author of text-books, 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 leakage through technical channels. e-mail: eryshov@mail.ru .*

Andrey Sergeevich Korsunky, *Candidate of Engineering, graduated from the Faculty of Radio-Communications at the 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.*

Abstract
The article studies an aspect of information opposition – monitoring of information security in information and telecommunications systems, and deals with a model of information security in information and telecommunication systems on basis of the Markovian-process theory.

Key words: monitoring of information security, information and telecommunication system, Markovian processes.

Введение

На современном этапе развития информационных технологий и прогрессивного роста потребностей общества в мультисервисных услугах, предоставляемых информационно-телекоммуникационными системами, необходимо повышать эффективность использования информационных ресурсов. В связи с этим резко возрастает значимость проблемы информационного обеспечения всех сфер деятельности.

Эта проблема может быть решена путем создания систем управления ИТКС, построенных на современных технологиях управления и соответствующих математических моделях. Одной из важнейших составляющих таких систем является подсистема управления безопасностью информации в распределенных ИТКС.

Модель процесса мониторинга безопасности информации

Управление безопасностью информации обеспечивает защиту всех процессов, происходящих в ИТКС, от несанкционированного доступа к информации, перехвата, уничтожения и модификации данных, расшифровки паролей и идентификаторов пользователей, искусственного прерывания сеансов взаимодействия прикладных процессов.

Процесс обеспечения безопасности информации в системе управления распределенными ИТКС будет эффективен при решении следующих основных задач:

– защита информации, циркулирующей в элементах ИТКС: автоматизированных системах (АС), локальных вычислительных сетях (ЛВС), узлах и линиях связи, – от внешних и внутренних угроз;

– мониторинг безопасности информации, циркулирующей в элементах и в ИТКС в целом.

Под мониторингом безопасности информации понимается комплекс организационных и технических мероприятий, направленных на проверку соответствия эффективности защиты установленным требованиям и/или нормам и принятие решений о повышении эффективности защиты в случае несоответствия требованиям.

Мониторинг безопасности информации в элементах и ИТКС в целом необходимо осуществлять на следующих четырех уровнях [1]:

– уровне прикладного программного обеспечения (ПО) ЭВМ элементов ИТКС;

– уровне систем управления базами данных (СУБД) элементов ИТКС;

– уровне операционных систем (ОС) ЭВМ элементов ИТКС;

– уровне сети, отвечающем за взаимодействие элементов ИТКС.

Как процесс мониторинг безопасности информации обладает следующими свойствами: непрерывность, объективность, полнота.

Для исследования процесса мониторинга безопасности информации в распределенных ИТКС и повышения его эффективности актуальной является задача построения его математической модели с целью выявления вероятностно-временных зависимостей его событий и состояний. Для решения данной задачи в частности применим аппарат теории Марковских случайных процессов.

Процесс мониторинга безопасности информации 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 [2].

Будем полагать, что переходы из одного состояния в другое происходят под воздействием пуассоновских потоков событий [2, 3].

Ориентированный граф состояний процесса мониторинга безопасности информации, описанного в терминах Марковских процессов [4] с дискретными состояниями и непрерывным временем, представлен на рисунке 1.

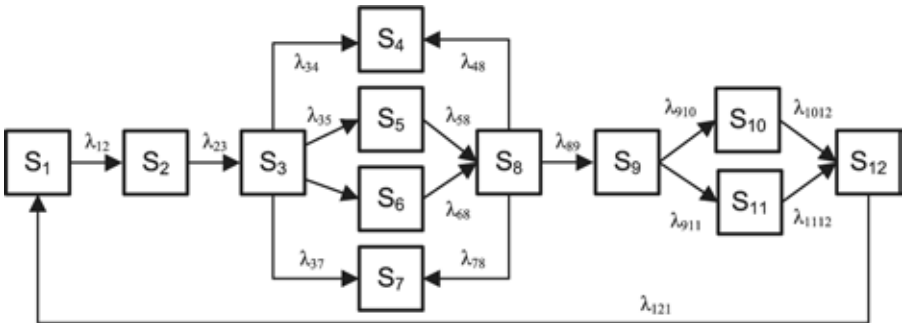

Рис. 1. Ориентированный граф состояний мониторинга безопасности информации в распределенных ИТКС

Описания состояний, входных и выходных потоков событий исследуемого процесса представлены в таблице.

Таблица

Описание состояний процесса мониторинга безопасности информации в распределенных ИТКС

№ п/п	Наименование состояния	№ вх. соб.	№ вых. соб.
S_1	Сбор данных: сканирование портов контролируемого оборудования элементов ИТКС	λ_{121}	λ_{12}
S_2	Сбор данных: идентификация сетевых маршрутов, сетевого и узлового оборудования элементов ИТКС	λ_{12}	λ_{23}
S_3	Сбор данных: идентификация служб и программного обеспечения ЭВМ элементов ИТКС	λ_{23}	λ_{34}, λ_{35}, λ_{36}, λ_{37}
S_4	Мониторинг безопасности информации на сетевом уровне ИТКС	λ_{34}	λ_{48}
S_5	Мониторинг безопасности информации на уровне операционных систем ЭВМ элементов ИТКС	λ_{35}	λ_{58}
S_6	Мониторинг безопасности информации на уровне прикладного программного обеспечения ЭВМ элементов ИТКС	λ_{36}	λ_{67}
S_7	Мониторинг безопасности информации на уровне систем управления базами данных элементов ИТКС	λ_{67}	λ_{78}
S_8	Декодирование и фильтрация собранных данных о контролируемых элементах ИТКС	λ_{48}, λ_{58}, λ_{68}, λ_{78}	λ_{89}
S_9	Семантический и статистический анализ собранных данных о контролируемых элементах ИТКС	λ_{89}	λ_{910}, λ_{911}
S_{10}	Обнаружение уязвимостей в контролируемых элементах ИТКС	λ_{910}	λ_{1012}
S_{11}	Отсутствие уязвимостей в контролируемых элементах ИТКС	λ_{911}	λ_{1112}
S_{12}	Принятие системой управления решений относительно того или иного действия по локализации, устранению обнаруженных уязвимостей в контролируемых элементах ИТКС	λ_{1012}, λ_{1112}	λ_{121}

Для получения вероятностных и временных характеристик процесса контроля безопасности информации для графа, представленного на рисунке 1, была составлена система обыкновенных дифференциальных уравнений Колмогорова [2].

$$
\begin{cases}
\dfrac{dp_1(t)}{dt} = p_{12}(t)\lambda_{121}(t) - p_1(t)\lambda_{12}(t), \\
\dfrac{dp_2(t)}{dt} = p_1(t)\lambda_{12}(t) - p_2(t)\lambda_{23}(t), \\
\dfrac{dp_3(t)}{dt} = p_2(t)\lambda_{23}(t) - p_3(t) \\
\qquad \{\lambda_{34}(t) + \lambda_{35}(t) + \lambda_{36}(t) + \lambda_{37}(t)\}, \\
\dfrac{dp_4(t)}{dt} = p_3(t)\lambda_{34}(t) - p_4(t)\lambda_{48}(t), \\
\dfrac{dp_5(t)}{dt} = p_3(t)\lambda_{35}(t) - p_5(t)\lambda_{58}(t), \\
\dfrac{dp_6(t)}{dt} = p_3(t)\lambda_{36}(t) - p_6(t)\lambda_{68}(t), \\
\dfrac{dp_7(t)}{dt} = p_3(t)\lambda_{37}(t) - p_7(t)\lambda_{78}(t), \\
\dfrac{dp_8(t)}{dt} = p_4(t)\lambda_{48}(t) + p_5(t)\lambda_{58}(t) + p_6(t)\lambda_{68}(t) + \\
\qquad + p_7(t)\lambda_{78}(t) - p_8(t)\lambda_{89}(t), \\
\dfrac{dp_9(t)}{dt} = p_8(t)\lambda_{89}(t) - p_9(t)\{\lambda_{910}(t) + \lambda_{911}(t)\}, \\
\dfrac{dp_{10}(t)}{dt} = p_9(t)\lambda_{910}(t) - p_{10}(t)\lambda_{1012}(t), \\
\dfrac{dp_{11}(t)}{dt} = p_9(t)\lambda_{911}(t) - p_{11}(t)\lambda_{1112}(t), \\
\dfrac{dp_{12}(t)}{dt} = p_{10}(t)\lambda_{1012}(t) + p_{11}(t)\lambda_{1112}(t) - \\
\qquad - p_{12}(t)\lambda_{121}(t),
\end{cases}
$$

$$\sum_i^{12} p_i(t) = 1.$$

Решение системы уравнений Колмогорова (1) было получено с помощью пакета математического программирования «Mathcad». Полученные в результате моделирования вероятностные и временные зависимости представлены на рисунке 2.

Из анализа полученных результатов видно как изменяются состояния процесса мониторинга безопасности информации в элементах ИТКС. Так, например, при $t = 0{,}001$ модельной единицы система мониторинга находится с максимальной вероятностью $P_1 = 0{,}4$ в состоя-

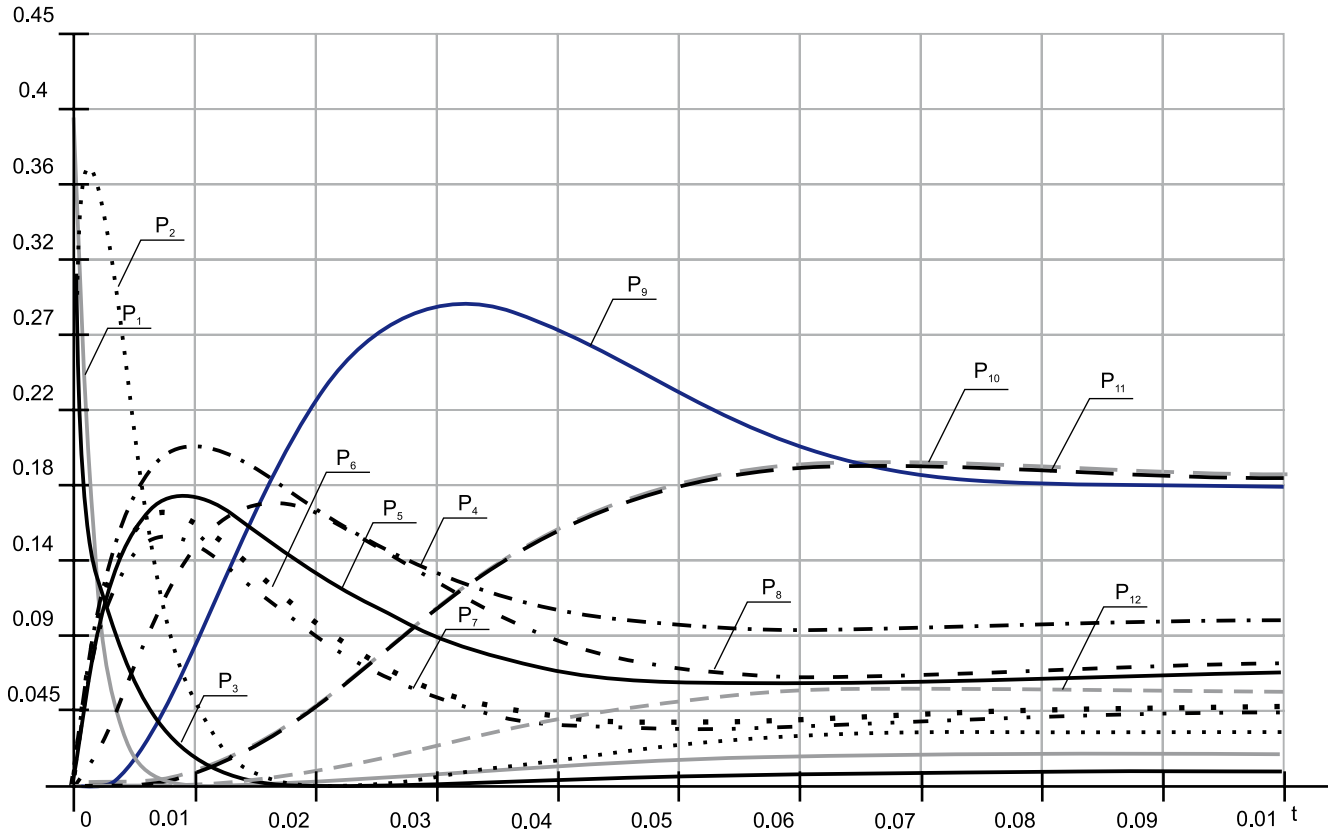

Рис. 2. Вероятностно-временные зависимости состояний процесса мониторинга безопасности информации в распределенных ИТКС

нии сбора данных – сканирования портов контролируемого оборудования элементов ИТКС. Далее при $t = 0,01$ модельной единицы система мониторинга находится с максимальной вероятностью $P_4 = 0,2$ в состоянии мониторинга безопасности информации на сетевом уровне ИТКС. Затем при $t = 0,03$ модельной единицы система мониторинга переходит в состояние семантического и статистического анализа собранных данных о контролируемых элементах ИТКС ($P_9 = 0,3$).

Начиная с момента времени наблюдаемого периода $t = 0,08$ модельной единицы процесс мониторинга безопасности информации в элементах ИТКС становится стационарным процессом с финальными вероятностями $P_i(t) = P_i = const$ и с максимальной вероятностью $P_{ЗАЩ} = P_{11} = 0,19$, т. е. система мониторинга безопасности информации в ИТКС подтверждает отсутствие уязвимостей в контролируемых элементах ИТКС.

Заключение

Таким образом, разработанная модель процесса мониторинга безопасности информации в ИТКС, 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 исследуемого процесса.

Выявленные в предлагаемой модели и полученные в результате проведенного моделирования зависимости послужат в дальнейшем основой для анализа существующих и синтеза новых систем мониторинга безопасности информации в ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. Липатников В.А., Стародубцев Ю.И. Информационная безопасность телекоммуникационных систем. – СПб. : ВУС, 2002. – 476 с.

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

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

4. Тихонов В.И., Миронов М.А. Марковские процессы. – М. : Сов. Радио, 1977. – 488 с.