

**В.А. Минаев<sup>1</sup>, И.Д. Королев<sup>2</sup>, В.В. Мухортов<sup>2</sup>**

(<sup>1</sup>МГТУ им. Н.Э. Баумана, Академия ГПС МЧС России, <sup>2</sup>Краснодарское высшее военное училище;  
e-mail: m1va@yandex.ru)

## **МАРКОВСКИЕ МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ БЕСПИЛОТНЫХ РОБОТОТЕХНИЧЕСКИХ ОБЪЕКТОВ**

*Анализируются процессы, протекающие в беспилотных робототехнических системах в условиях злонамеренных программно-аппаратных воздействий на них, представляемые в виде однородной марковской цепи.*

*Ключевые слова: модель, марковский процесс, беспилотник, активное обнаружение информационной атаки, активное противодействие атаке.*

**V.A. Minaev, I.D. Korolev, V.V. Muxortov**

## **MARKOV MODELS OF DRONES INFORMATION SYSTEMS PROTECTION**

*Processes occurring in drone robotic systems in conditions of malicious program and apparatus impacts on them, represented as a homogeneous Markov chain are analyzed.*

*Key words: model, Markov process, drone, active detection of information attack, active opposition to attack, emergency.*

Статья поступила в редакцию Интернет-журнала 18 ноября 2016 г.

### **Введение**

В последние годы растут количество и области применения беспилотных робототехнических систем (БРС) в деятельности подразделений МЧС (операции по спасению людей в чрезвычайных ситуациях, связанных с обрушением сооружений и зданий, разведка обстановки при паводках и лесных пожарах и другие задачи), вооружённых сил России и других ведомств, заинтересованных в высокотехнологичном решении различных мониторинговых, поисковых, разведывательных и других оперативно-тактических задач. Одновременно с увеличением масштабов применения БРС растут угрозы и безопасности их функционирования [1] в результате возникновения уязвимостей [2] и проведении злонамеренных программно-аппаратных воздействий (ПАВ) [3-5].

Очевидно, что потеря БРС – это не только утрата важнейшего, другими способами невозполнимого источника информации, но и потеря огромных финансовых ресурсов, израсходованных на создание беспилотника. Поэтому разработка современных математических моделей и программно-аппаратных средств обеспечения информационной защиты дронов выступает актуальной научной и практической задачей.

## Система вложенных моделей функционирования защиты БРС

Для описания функционирования БРС наиболее адекватным является математическое описание с использованием марковского случайного процесса [4]. Начнем с простейшей марковской модели.

Функционирование БРС представляется в виде графа конечных состояний (рис. 1), где –  $S_1$  – БРС работоспособна, ПАВ отсутствуют,  $S_2$  – БРС работоспособна, ПАВ блокированы,  $S_3$  – БРС не работоспособна, принимаются меры по её восстановлению, а  $\lambda_{mn}(t)$  ( $m, n = 1, 2, 3$ ) – интенсивности переходов из состояния  $m$  в состояние  $n$ .

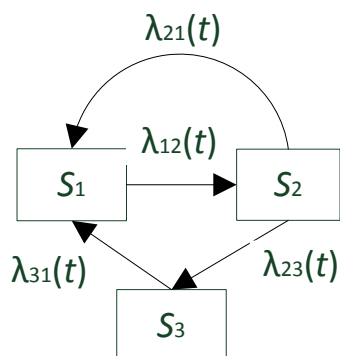


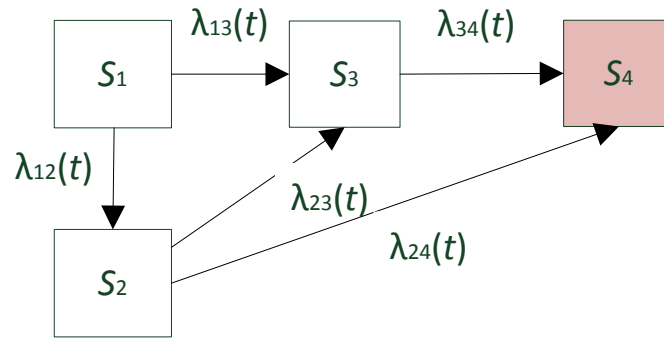
Рис. 1. Начальный граф состояний БРС

Простейшая модель функционирования БРС (рис.1) представляется в виде системы дифференциальных уравнений (1) с учётом уравнения нормировки:

$$\begin{cases} \frac{dp_1(t)}{dt} = -\lambda_{12} \cdot p_1(t) + \lambda_{21} \cdot p_2(t) + \lambda_{31} \cdot p_3(t); \\ \frac{dp_2(t)}{dt} = -(\lambda_{21} + \lambda_{23}) \cdot p_2(t) + \lambda_{12} \cdot p_1(t); \\ \frac{dp_3(t)}{dt} = -\lambda_{31} \cdot p_3(t) + \lambda_{23} \cdot p_2(t); \\ \sum_{i=1}^3 p_i(t) = 1. \end{cases} \quad (1)$$

В модели (1) не рассматриваются процессы обнаружения и противодействия ПАВ, поэтому продолжим усложнять модель.

С учётом проведения злонамеренных ПАВ однородная марковская поглощающая цепь представляется в виде графа, показанного на рис. 2, где  $S_1$  – БРС работоспособна, не атакована,  $S_2$  – БРС работоспособна, атакована, факт атаки не установлен,  $S_3$  – БРС неработоспособна, атакована, факт атаки не установлен,  $S_4$  – БРС неисправна, полная потеря контроля, а  $\lambda_{mn}(t)$  ( $m, n = 1, 2, 3, 4$ ) – интенсивности переходов из состояния в состояние.



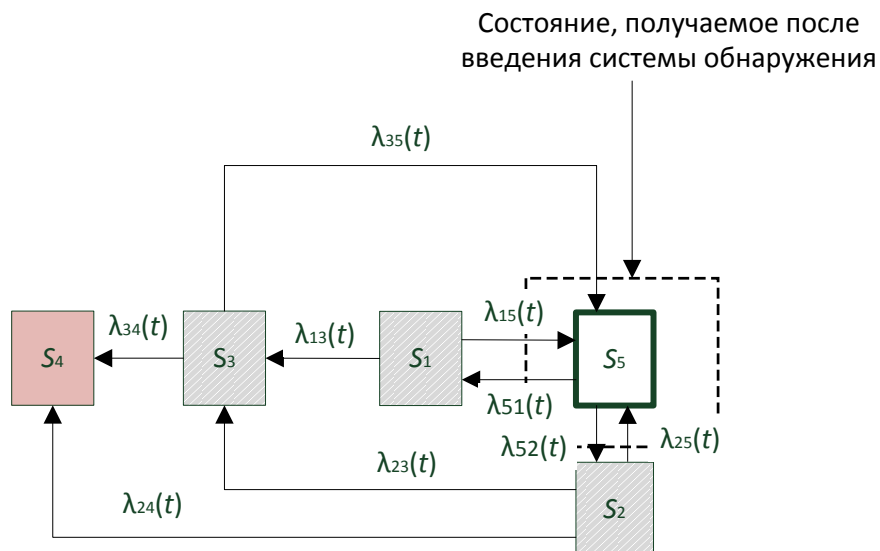
**Рис. 2.** Граф состояния БРС, функционирующей в условиях проведения ПАВ

Предложенная на рис. 2 графовая модель функционирования БРС представляется (с учётом уравнения нормировки) в виде системы дифференциальных уравнений, результатом решения которой является аналитические соотношения вероятностей устойчивого функционирования в условиях проведения ПАВ:

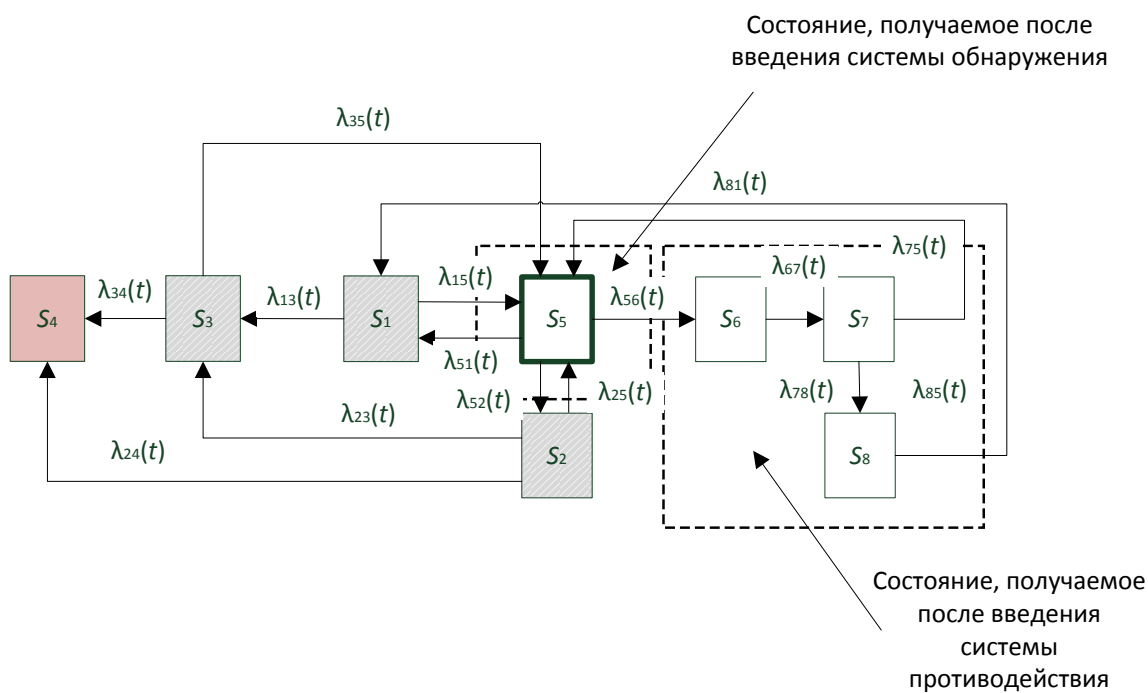
$$\begin{cases} \frac{dp_1(t)}{dt} = -(\lambda_{12} + \lambda_{13})p_1(t); \\ \frac{dp_2(t)}{dt} = \lambda_{12}p_1(t) - (\lambda_{23} + \lambda_{24})p_2(t); \\ \frac{dp_3(t)}{dt} = \lambda_{13}p_1(t) + \lambda_{23}p_2(t) - \lambda_{34}p_3(t); \\ \frac{dp_4(t)}{dt} = \lambda_{34}p_3(t) + \lambda_{24}p_2(t); \\ \sum_{i=1}^4 p_i(t) = 1. \end{cases} \quad (2)$$

С введением системы активного обнаружения атак функционирование БРС примет следующее описание (рис. 3), где –  $S_1$  – БРС работоспособна, не атакована,  $S_2$  – БРС работоспособна, атакована, факт атаки не установлен,  $S_3$  – БРС неработоспособна, атакована, факт атаки не установлен,  $S_4$  – БРС неисправна, полная потеря контроля,  $S_5$  – осуществляется контроль осуществления атаки, а  $\lambda_{mn}(t)$  ( $m, n = 1, 2, 3, 4, 5$ ) – интенсивности переходов из состояния в состояние.

Далее при введении системы противодействия ПАВ граф приобретает вид, показанный на рис. 4. Он позволяет сформировать модель функционирования БРС с введенными состояниями, учитывающими противодействия атакам, где –  $S_1$  – БРС работоспособна, не атакована,  $S_2$  – БРС работоспособна, атакована, факт атаки не установлен,  $S_3$  – БРС неработоспособна, атакована, факт атаки не установлен,  $S_4$  – БРС неисправна, полная потеря контроля,  $S_5$  – осуществляется контроль наличия атаки,  $S_6$  – факт атаки установлен, ведётся поиск решения,  $S_7$  – осуществление активного противодействия атаке,  $S_8$  – восстановление системы БРС после атаки, в случае невозможности активного противодействия ей, а  $\lambda_{mn}(t)$  – интенсивности переходов из состояния в состояние.



**Рис. 3.** Граф состояний БРС при введении активной системы обнаружения ПАВ



**Рис. 4.** Граф состояний БРС при введении системы обнаружения и противодействия ПАВ

Конечная модель функционирования БРС, учитывающая проведение злонамеренных нападений на БРС и защиту от нападений, представляется в виде системы дифференциальных уравнений (3).

Наибольшее количество входов/выходов в модели БРС (2) приходится на состояние  $S_5$ , что свидетельствует о его основной роли при построении систем защиты информации в беспилотных робототехнических комплексах.

Результатом решения системы дифференциальных уравнений выступают аналитические соотношения для каждого из состояний функционирования БРС.

Рассматривая системы дифференциальных уравнений в начальной (2) и конечных (3) системах можно увидеть, что вероятность наступления состояния поглощения  $S_4$  (рис. 2, 3 и 4) зависит только от предшествующих состояний, таким образом, разрабатываемые системы защиты БРС от ПАВ должны быть направлены на минимизацию вероятностей переходов в состояния  $S_2$  и  $S_3$ .

$$\left\{ \begin{array}{l} \frac{dp_1(t)}{dt} = \lambda_{51}p_5(t) + \lambda_{81}p_8(t) - (\lambda_{13} + \lambda_{15})p_1(t); \\ \frac{dp_2(t)}{dt} = \lambda_{52}p_5(t) - (\lambda_{23} + \lambda_{24} + \lambda_{25})p_2(t); \\ \frac{dp_3(t)}{dt} = \lambda_{13}p_1(t) + \lambda_{23}p_2(t) - (\lambda_{34} + \lambda_{35})p_3(t); \\ \frac{dp_4(t)}{dt} = \lambda_{34}p_3(t) + \lambda_{24}p_2(t); \\ \frac{dp_5(t)}{dt} = \lambda_{15}p_1(t) + \lambda_{25}p_2(t) + \lambda_{35}p_3(t) + \lambda_{794}p_7(t) - (\lambda_{51} + \lambda_{52} + \lambda_{56})p_5(t); \\ \frac{dp_6(t)}{dt} = \lambda_{56}p_5(t) - \lambda_{67}p_2(t); \\ \frac{dp_7(t)}{dt} = \lambda_{67}p_6(t) - (\lambda_{75} + \lambda_{78})p_7(t); \\ \frac{dp_8(t)}{dt} = \lambda_{78}p_8(t) - \lambda_{81}p_8(t); \\ \sum_{i=1}^8 p_i(t) = 1. \end{array} \right. \quad (3)$$

### Выводы

Обсуждаемая в статье система моделей функционирования БРС в условиях проведения ПАВ достаточно полно раскрывает состояния информационной защиты беспилотников. Указанная система представляет собой последовательно усложняющиеся модели БРС: пассивный режим функционирования – активное обнаружение информационной атаки – активное противодействие атаке. В зависимости от важности мониторинговых, поисково-спасательных, разведывательных и других оперативно-тактических задач, решаемых с помощью беспилотников подразделениями МЧС и других служб, использующих дроны, а также от финансового обеспечения указанных высокотехнологичных проектов, на этой основе может строиться программно-аппаратная база БРС для создания эффективных систем обнаружения и противодействия злонамеренным воздействиям на беспилотные робототехнические системы.

## Литература

1. **ГОСТ** Р.50.1.053-2005. "Основные термины и определения в области технической защиты информации".
2. **Банк** данных угроз безопасности информации. <http://bdu.fstec.ru>. Дата обращения 10.10.16.
3. **Мухортов В.В., Королев И.Д.** Защита беспилотных летательных аппаратов от внешних программно-аппаратных воздействий // Сборник статей по материалам XXXII международной научно-практической конференции "Наука вчера, сегодня, завтра". № 3 (25). Новосибирск: изд. АНС "СибАК", 2016. С. 87-95.
4. **Карпычев В.Ю., Минаев В.А.** Цена информационной безопасности // Системы безопасности. 2003. № 5. С. 128-130.
5. **Минаев В.А., Фисун А.П., Скрыль С.В. и др.** Информатика. Средства и системы обработки данных. Серия "Информатика и информационная безопасность": учебник. М.: Маросейка, 2008. 544 с.
6. **Вентцель Е.С., Овчаров Л.А.** Теория случайных процессов и её инженерные приложения: учеб. пособие. 5-е изд. М.: КНОРУС, 2011. 448 с.