УДК 519.876.5

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВОЗДЕЙСТВИЯ УГРОЗ НА ИНФОРМАЦИОННУЮ СИСТЕМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

[1]Шувалов И.А., [2]Семенчин Е.А.

[1]Управление ГИБДД ГУ МВД России по Краснодарскому краю, Краснодар, e-mail: ilya_kizlyar@mail.ru;
[2]ФГБОУ ВПО «Кубанский государственный университет», Краснодар, e-mail: es14@mail.ru

В работе предложена математическая модель воздействия внутренних и внешних угроз на информационную систему обработки персональных данных «Информационные ресурсы Управления ГИБДД», используемую в служебной деятельности сотрудниками Управления государственной инспекцией безопасности дорожного движения Главного управления Министерства внутренних дел России по Краснодарскому краю. Поэтапно описан процесс построения двух математических моделей информационной системы: а) с помощью марковской цепи с непрерывным временем; б) с помощью марковской цепи с дискретными моментами перехода из одного состояния в другое. Предложена методика выявления актуальных угроз безопасности персональных данных при их обработке в рассматриваемой информационной системе. Приведены примеры расчетов вероятностей нахождения математической модели информационной системы в одном из трех рассматриваемых состояний (угроза не наступила, угроза наступила, но не была реализована, и угроза реализована).

Ключевые слова: математическое моделирование, угрозы безопасности, безопасность персональных данных

MATHEMATICAL MODEL OF IMPACT OF THREATS ON INFORMATION SYSTEM OF PROCESSING OF PERSONAL INFORMATION

[1]Shuvalov I.A., [2]Semenchin E.A.

[1]Control of traffic police of Head department of the Ministry of Internal Affairs of Krasnodar Krai, Krasnodar, e-mail: ilya_kizlyar@mail.ru;
[2]Kuban State University, Krasnodar, e-mail: es14@mail.ru

In article the mathematical model of implementation of security risks of one of segments of an information system of processing of personal data «Information resources of Management of traffic police» is offered. The system is used in the official activities by employees of Management by State Inspection for Road Traffic Safety of Head department of the Ministry of Internal Affairs of Russia for Krasnodar Krai. Process of creation of two mathematical models of information system is described: by means of a Markov chains with continuous time; b) using a Markov chain with discrete moments of transition from one state to another. The technique of identification of actual threats of safety of personal information during their processing in the information system is offered. Examples of calculations of probabilities of stay of mathematical model of information system in one of three considered conditions are given (threat didn't come, threat came, but it wasn't realized, and threat is realized).

Keywords: mathematical modeling, security risks, safety of personal data

В статьях [10, 11] предложена имитационная модель функционирования сегментов информационной системы «Информационные ресурсы Управления ГИБДД», используемой в повседневной деятельности сотрудниками УГИБДД ГУ МВД по Краснодарскому краю и подчиненными ему подразделениями. С помощью этой модели можно определить (выявить) угрозы, которые представляют реальную опасность для информационной системы. Однако, используя статистические данные, можно определить такие угрозы также методами математического моделирования.

Цель данной работы – предложить математическую модель воздействия угроз на указанную информационную систему и на основе этой модели разработать методику их выявления.

Рассматриваемую информационную систему можно интерпретировать как систему массового обслуживания, в которую поступают угрозы (заявки). Вначале рассмотрим ситуацию, когда на вход системы поступают угрозы одного типа, предполагая при этом, что данная угроза не может быть реализована или наступить несколько раз в один и тот же момент времени. Если выполнены указанные предположения, то система может находиться в трёх различных состояниях (рис. 1):

1) угроза не поступала, а значит, не была реализована;

2) угроза поступала, но не была реализована;

3) угроза поступала и была реализована.

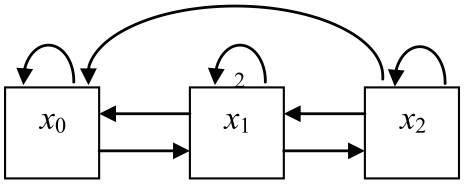

Рис. 1. Ориентированный граф

Модель системы, которая может находиться в указанных состояниях, предложена в работах А.П. Росенко [7, 9]. В данных ра-

ботах допускалось наличие поглощающих состояний системы и выполнение требования: система не может находиться в одном состоянии в течении некоторого отрезка времени. Указанные допущения не позволяют использовать предложенную в [7, 9] математическую модель для анализа информационной системы «Информационные ресурсы УГИБДД», потому что, как показал анализ многолетних наблюдений, у системы поглощающие состояния отсутствуют: реализация угрозы либо никак не влияет на работоспособность системы в целом, либо может вывести из строя на непродолжительный промежуток времени один из её сегментов. Если же учитывать возможность возврата системы в исходное состояние, то можно будет изучить её поведение на протяжении длительного промежутка времени.

Математическая модель информационной системы «Информационные ресурсы УГИБДД»

Рассматриваемая система является системой с восстановлением, так как состояние x_2 не является поглощающим, а значит, система может вернуться из x_2 в исходное состояние. Будем рассматривать систему с непрерывным временем. Переход из состояния в состояние в системе осуществляется согласно ориентированному графу, представленному на рис. 1. Для описания процесса перехода из состояния в состояние построим матрицу интенсивностей перехода [1]

$$p_{ij} = \begin{vmatrix} \lambda_{11} & \lambda_{12} & 0 \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} \end{vmatrix}. \quad (1)$$

Из предыдущих соглашений следует, что элементы этой матрицы должны удовлетворять условиям:

$$\begin{aligned} \lambda_{12} &= -\lambda_{11}; \\ \lambda_{22} &= -\lambda_{21} - \lambda_{23}; \\ \lambda_{33} &= -\lambda_{31} - \lambda_{32}. \end{aligned} \quad (2)$$

Требования (2) необходимы для выполнения условий, предъявляемых к элементам матрицы интенсивностей [1]:

$$\sum_{j=1}^{n} \lambda_{ij} = 0, \ (i = \overline{1, n}).$$

Элементы матрицы интенсивностей переходов могут быть найдены (вычислены) с помощью имитационной модели, предложенной в [11]. В данной работе опишем вероятностно-аналитический способ их определения. Согласно [1], в соответствии с видом информационной системы (см. рис. 1), для определения вероятностей $p_0(t)$, $p_1(t)$, $p_2(t)$ имеем систему дифференциальных уравнений

$$\begin{cases} \dfrac{dp_0(t)}{dt} = p_0(t)\lambda_{11} + p_1(t)\lambda_{21} + p_2(t)\lambda_{31}, \\ \dfrac{dp_1(t)}{dt} = p_0(t)\lambda_{12} + p_1(t)\lambda_{22} + p_2(t)\lambda_{32}, \\ \dfrac{dp_2(t)}{dt} = p_1(t)\lambda_{23} + p_2(t)\lambda_{33} \end{cases} \quad (3)$$

с начальными условиями

$$p_0(0) = 1; \ p_1(0) = 0; \ p_2(0) = 0. \quad (4)$$

Задачу Коши (3), (4), представляющую собой математическую модель рассматриваемой информационной системы, можно решить численно, если воспользоваться известными пакетами прикладных программ (например, пакетом «Mathcad», разработанным фирмой Parametric Technology Corporation).

Если моменты времени перехода t являются дискретными, то есть переход системы из состояния в состояние осуществляется в строго определенный момент времени, матрица вероятностей перехода из состояния в состояние за один шаг имеет вид (1), матрица вероятностей перехода за n шагов (в момент $t = n$) – следующий вид [3, 9]:

$$\left\| p_{ij}(n) \right\| = \begin{vmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} \end{vmatrix}^n. \quad (5)$$

Так как $p(0) = (1, 0, 0)$ (см. 4) задан, то вектор абсолютных вероятностей $p(n) = (p_0(n), p_1(n), (p_2(n))$ определяется соотношением

$$p(n) = p(0) \left\| p_{ij}(n) \right\|. \quad (6)$$

Примеры численной реализации непрерывной и дискретной моделей

Пример 1. Пусть матрица интенсивностей перехода (1) имеет вид:

$$\begin{vmatrix} -0,075 & 0,075 & 0 \\ 0,825 & -0,85 & 0,025 \\ 0,875 & 0 & -0,875 \end{vmatrix}.$$

Построим решение задачи (3), (4) методом Рунге–Кутты четвертого порядка для момента времени $t = 50$ с количеством шагов 4 на каждую единицу времени (рис. 2), воспользовавшись пакетом прикладных программ «MathCad».

В результате проведенных вычислений найдены значения вероятностей $p_0(t)$, $p_1(t)$, $p_2(t)$ для различных моментов времени, которые представлены в табл. 1

Таблица 1

Результаты вычислений значений $p_0(t)$, $p_1(t)$, $p_2(t)$ для различных моментов времени

Значение времени t	Вероятность нахождения системы в состоянии x_0	Вероятность нахождения системы в состоянии x_1	Вероятность нахождения системы в состоянии x_2
1	0,951	0,049	0
2	0,93	0,069	0,001
3	0,922	0,076	0,002
4	0,919	0,079	0,002
5	0,918	0,08	0,002
6	0,917	0,081	0,002
…	…	…	…
25	0,917	0,081	0,002
…	…	…	…
50	0,917	0,081	0,002

Следовательно, в момент времени $t = 50$ $p_0(t) = 0,917$, $p_1(t) = 0,081$, $p_2(t) = 0,002$.

В соответствии с данными, приведенными в табл. 1, построим график изменения значений вероятностей нахождения системы в одном из состояний в зависимости от времени t (рис. 2).

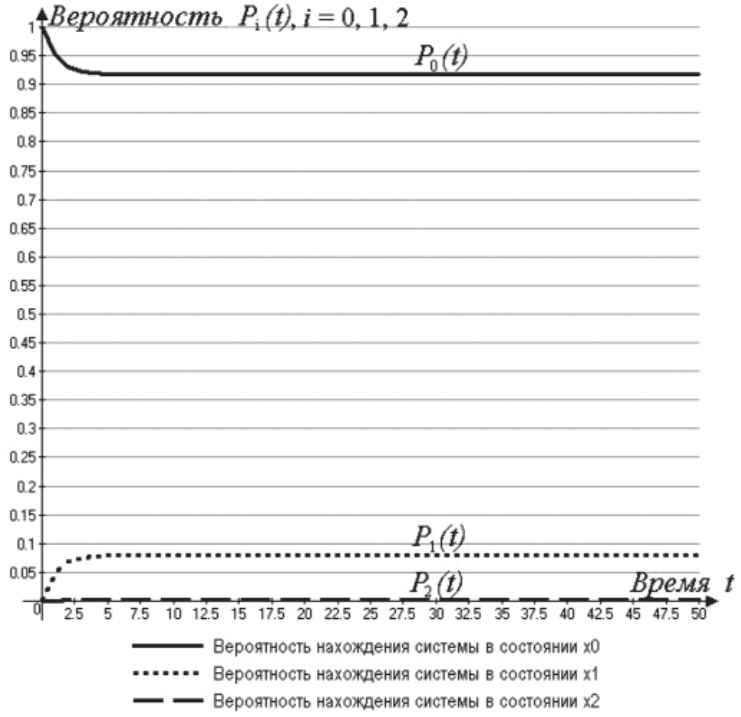

Рис. 2. График изменения значений вероятностей $p_i(t)$, $i = 0, 1, 2$ в зависимости от времени t

Пример 2. Пусть моменты перехода t системы из состояния в состояние являются дискретными ($t = n$, $n = 1, \ldots, 8$), а матрица вероятностей перехода за один шаг имеет вид:

$$\left\| p_{ij} \right\| = \begin{vmatrix} 0{,}9 & 0{,}1 & 0 \\ 0{,}9075 & 0 & 0{,}0025 \\ 1 & 0 & 0 \end{vmatrix},$$

начальное распределение:

$$p(0) = (1{,}0{,}0).$$

Вычислим вероятности нахождения системы в каждом из состояний x_i, $i = 0, 1, 2$, через 8 шагов, воспользовавшись пакетом прикладных программ «MathCad». Результаты вычислений представлены в табл. 2.

Таблица 2

Результаты вычислений, полученные с использованием программного обеспечения «MathCad»

Шаг эксперимента	Вероятность нахождения системы в состоянии x_0	Вероятность нахождения системы в состоянии x_1	Вероятность нахождения системы в состоянии x_2
1	0,9	0,1	0
2	0,88	0,1	0,02
3	0,864	0,108	0,028
4	0,856	0,111	0,033
5	0,852	0,113	0,035
6	0,849	0,114	0,037
7	0,848	0,115	0,038
8	0,847	0,115	0,038

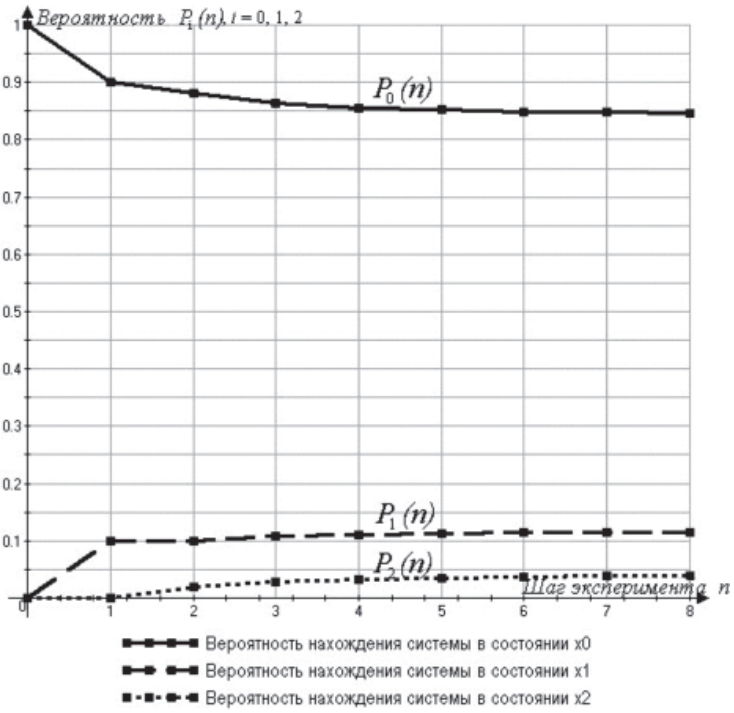

Рис. 3. График изменения значений вероятностей $p_i(t)$, $i = 0, 1, 2$ в зависимости от шага эксперимента n

По данным табл. 2 построен график изменения значений вероятностей $p_0(t)$, $p_1(t)$, $p_2(t)$ (рис. 3):

Заключение

В работе предложена математическая модель реализации угроз безопасности информационной системы «Информационные ресурсы УГИБДД», а также методика выявления актуальных угроз безопасности исследуемой системы, разработанная на основе этой модели.

Примеры численных результатов анализа модели с помощью предложенной ме-

тодики показывают, что их использование позволяет выделить угрозы, которые являются актуальными для рассматриваемой информационной системы и могут использоваться на практике. Недостатком предложенной методики является необходимость рассмотрения поведения модели системы при воздействии на неё отдельно каждого типа угроз и невозможность изучения поведения при воздействии нескольких угроз одновременно. Вместе с тем, изучение поведения модели при воздействии на неё каждой угрозы в отдельности позволяет более детально изучить каждый тип угрозы и выделить те, вероятность наступления которых является наиболее высокой.

Список литературы

1. Алиев Т.И. Основы моделирования дискретных систем: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 363 с.

2. Вентцель Е.С. Теория вероятностей. – М.: Наука, 1969. – 576 с.

3. Волков И.К., Зуев С.М., Цветкова Г.М. Случайные процессы: учебник для вузов / под ред. В.С. Зарубина, А.П. Крищенко. – М.: МГТУ им.Баумана, 1999. – 448 с.

4. Зыков С.В. Введение в теорию программирования. Функциональный подход. – Учебный Центр безопасности информационных технологий Microsoft МИФИ, 2003.

5. Калиткин Н.Н. Численные методы. – М.: Наука, 1978. – 512 с.

6. Кирьянов Д.В. Самоучитель Mathcad 11. – СПб.: БХВ-Петербург, 2003. – 560 с.: ил.

7. Росенко А.П. Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе Известия ЮФУ. Технические науки. Тематический выпуск. «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2008. – № 8 (85).

8. Солодов А.П., Очков В.Ф. Mathcad/Дифференциальные модели. – М.: Издательство МЭИ, 2002. – 239 с.: ил.

9. Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации: монография / А.П. Росенко. – М.: Гелиос АРВ, 2008. – 154 с.

10. Шувалов И.А., Росенко А.П. Имитационная модель реализации внутренних и внешних угроз безопасности информационной системы на сегменте «коммутатор – сервер» // Вестник Дагестанского государственного университета. – 2013. – Вып. 1. – С. 112–123.

11. Шувалов И.А., Семенчин Е.А. Имитационная модель реализации внутренних и внешних угроз безопасности информационной системы на сегменте «Маршрутизатор – маршрутизатор» // Фундаментальные исследования. – 2012. – № 9. – С. 425–431.

References

1. Aliev T.I. Osnovy modelirovanija diskretnyh sistem: Uchebnoe posobie. SPb: SPbGU ITMO, 2009. 363 p.

2. Ventcel’ E.S. Teorija verojatnostej. M.: Nauka, 1969. 576 p.

3. Volkov I.K., Zuev S.M., Cvetkova G.M. Sluchajnye processy: Uchebnik dlja VUZov / Pod red. V.S. Zarubina, A.P. Krishhenko. M.: MGTU im.Baumana, 1999. 448 p.

4. Zykov S.V. Vvedenie v teoriju programmirovanija. Funkcional’nyj podhod. Uchebnyj Centr bezopasnosti informacionnyh tehnologij Microsoft MIFI, 2003.

5. Kalitkin N.N. Chislennye metody. M.: Nauka, 1978. 512 s.

6. Kir’janov D.V. Samouchitel’ Mathcad 11. SPb.: BHV-Peterburg, 2003. 560 s.: il.

7. Rosenko A.P. Matematicheskoe modelirovanie vlijanija vnutrennih ugroz na bezopasnost’ konfidencial’noj informacii, cirkulirujushhej v avtomatizirovannoj informacionnoj sisteme Izvestija JuFU. Tehnicheskie nauki. Tematicheskij vypusk. «Informacionnaja bezopasnost’». Taganrog: Izd-vo TTI JuFU, 2008. no. 8 (85).

8. Solodov A.P., Ochkov V.F. Mathcad/Differencial’nye modeli. M.: Izdatel’stvo MJeI, 2002. 239 p.

9. Teoreticheskie osnovy analiza i ocenki vlijanija vnutrennih ugroz na bezopasnost’ konfidencial’noj informacii: monografija / A.P. Rosenko. M.: Gelios ARV, 2008. 154 p.

10. Shuvalov I.A., Rosenko A.P. Imitacionnaja model’ realizacii vnutrennih i vneshnih ugroz bezopasnosti informacionnoj sistemy na segmente «kommutator server» / Vestnik Dagestanskogo gosudarstvennogo universiteta. 2013. Vyp. 1. pp. 112–123.

11. Shuvalov I.A., Semenchin E.A. Imitacionnaja model’ realizacii vnutrennih i vneshnih ugroz bezopasnosti informacionnoj sistemy na segmente «Marshrutizator marshrutizator» // Fundamental’nye issledovanija. 2012. no. 9. pp. 425–431.

Рецензенты:

Лебедев К.А., д.ф.-м.н., профессор кафедры прикладной математики, ФГБОУ ВПО «Кубанский государственный университет», г. Краснодар;

Приходько А.И., д.т.н., профессор кафедры общего, стратегического, информационного менеджмента и бизнес-процессов, ФГБОУ ВПО «Кубанский государственный университет», г. Краснодар.

Работа поступила в редакцию 15.08.2013.