Раздел I. Информационная безопасность

УДК 004.942, 51-74, 519.857.3

А.П. Росенко, И.В. Бордак

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПРЕДЕЛЕНИЯ ВЕРОЯТНОСТИ ПОСЛЕДСТВИЙ ОТ РЕАЛИЗАЦИИ ЗЛОУМЫШЛЕННИКОМ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

Целью работы является разработка математической модели определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения на основе Марковских случайных процессов (МСП) с непрерывным временем. Задачами исследования являются: дать определение МСП применительно к автоматизированной информационной системе (АИС); произвести описание МСП с непрерывным параметром; определить допущения, принятые при решении поставленной цели; описать граф состояния системы при воздействии на нее n *независимых потоков угроз и соответствующую ему матрицу состояний; обосновать необходимость применения дифференциальных уравнений Колмогорова для определения вероятностей перехода АИС в каждое возможное состояние, решение которых осуществлено с использованием прямого преобразования Лапласа; разработать частные случаи для получения финальных вероятностей, когда интенсивность воздействия угрозы равна интенсивности их парирования и когда на систему воздействует один поток угроз. На основе проведенных исследований: обоснована применимость МСП для оценки влияния различных угроз на безопасность конфиденциальной информации, разработаны математические методы исследования безопасности информации ограниченного распространения (ИОР) на основе Марковского случайного процесса с непрерывным параметром и математические методы с учетом воздействия на АИС* n *независимых потоков угроз, а также когда интенсивность парирования* i*-го потока угрозы* μ_i *равна интенсивности воздействия* i*-го потока угрозы* λ_i *и одной* i*-й угрозы (как частные случаи). Разработанные и обоснованные практические рекомендации при реализации собственниками информации ограниченного распространения обеспечат повышение защищенности информации, минимизацию материального ущерба за счет выбора оптимальных стратегий, применяемых методов и средств защиты ИОР. Предложенные методы и методики на основе МСП показали возможность количественной оценки безопасности ИОР, что позволит, используя полученные данные, разрабатывать научно-обоснованные организационно-профилактических мероприятий по повышению уровня защищенности информации ограниченного распространения, циркулирующей в различных структурных образованиях РФ. Разработанные математические модели, программное обеспечение и методики представлены в доступном виде для практического использования другими специалистами, занимающимися разработкой и применением аналогичного теоретического аппарата в других областях народного хозяйства.*

Безопасность информации; угрозы; математическая модель; математическое моделирование; Марковские случайные процессы.

A.P. Rosenko, I.V. Bordak

A MATHEMATICAL MODEL FOR DETERMINING THE PROBABILITY OF CONSEQUENCES FROM THE IMPLEMENTATION OF THE ATTACKER THREATS TO INFORMATION SECURITY LIMITED DISTRIBUTION

The Aim of this work is to develop a mathematical model for determining the likelihood and consequences from the implementation of the attacker threats to the security of restricted information on the basis of Markov random processes (SMEs) with continuous time. The objectives of the study are: to define SMEs in relation to automated information system (AIS); to produce a description of SMEs with a continuous parameter; identify the assumptions made when solving the goal; to describe the count state of the system when subjected to n independent streams of threats and corresponding the matrix of conditions; to justify application of the Kolmogorov differential equations for the determination of transition probabilities of AIS in each possible state, the solution of which is implemented using the direct Laplace transform; to develop particular cases to obtain the final probability, when the intensity of impact of a hazard is equal to the intensity of their parry and when the system operates a single stream of threats. On the basis of the research: the paper substantiates the applicability of SMEs to assess the impact of various threats on the security of confidential information, mathematical methods of investigation of the security KEY based on a random Markov process with a continuous parameter and mathematical methods taking into account the impact on AIS n independent streams of threats, and when the intensity parry flux and the threat of equal intensity flux and threats and one of the i-th threat (as special cases). Developed and informed practical recommendations for the implementation of the owners of restricted information would enhance the security of information, minimizing material damage due to the choice of optimal strategies, methods and remedies IOR. Proposed methods and techniques based on SMEs showed the possibility of quantitative assessment of security in the IOR, which will allow, using this data to develop evidence-based organizational and preventive measures on the improvement of the protection of restricted information, circulating in different structural entities of the Russian Federation. The developed mathematical model, software, and techniques presented in an understandable form for practical use other professionals engaged in developing and using similar theoretical apparatus in other areas of the economy.

Information security; threats; mathematical model; mathematical modeling; Markov random processes.

Введение. Безопасность (ИОР) является одной из важнейших характеристик, под которой понимают состояние защищенности (АИС), её относительно самостоятельных структурных элементов, при которой с требуемой вероятностью обеспечивается защита ИОР от утечки, хищения, утраты, уничтожения, искажения, копирования, блокирования и т.п. [1, 2, 4, 10, 17].

Известно, что безопасность ИОР обеспечивается на всех стадиях её жизненного цикла. Однако, с точки зрения соблюдения конфиденциальности информации, важнейшим этапом является этап использования ИОР по назначению. Исследования показывают, что именно на этом этапе имеет место наибольшее количество несанкционированных воздействий [2, 4]. В то же время анализ статистических данных показывает, что большинство случаев несанкционированного доступа к ИОР связаны с так называемыми антропогенными факторами [2, 6, 13]. В свою очередь антропогенные факторы обусловлены деятельностью или бездеятельностью человека, приводящей к преднамеренным или непреднамеренным ошибкам, как собственника, так и пользователей конфиденциальной информации. Это связано с нарушением правил обращения с конфиденциальной информацией, недостаточным уровнем знаний, умений и практических навыков по применению существующих средств и методов защиты информации. Указанные обстоятельства свидетельствуют о необходимости рассмотрения АИС как сложной человеко-машинной системы, для которой характерны признаки, присущие сложным системам [1, 2. 4].

Практика показывает, что оптимизация процесса обеспечения безопасности ИОР возможна на основе разработки новых, более современных защитных механизмов с учетом воздействия на человеко-машинную информационную систему различных угроз.

Это связанно с тем, что существующие методы и методики, применяемые для оценки безопасности ИОР, не ориентированы на получение количественных результатов. В связи с этим актуальной научной проблемой, обусловленной острой потребностью обеспечения безопасности ИОР, является разработка методов, адаптированных к процессам и явлениям, возникающим в человеко-машинных информационных системах и направленных на количественную оценку таких проявлений.

Как показано в [1, 2, 13, 19] в основу методов исследования безопасности ИОР может быть положено математическое описание процесса воздействия на АИС и её структурные элементы различных угроз, вследствие чего, система может переходить в различные состояния, обусловленные проявлением или не проявлением угроз, возникновением или не возникновением особой ситуации, нарушением безопасности ИОР, последствиями от реализации различных угроз и величиной ущерба, наносимого собственнику ИОР.

Понятие Марковского случайного процесса применительно к АИС. Пусть на АИС в произвольный момент времени t_i воздействует *i*-я угроза. В результате такого воздействия АИС переходит из состояния S_0 в состояние S_i. Представим процесс перехода АИС из S_0 – го состояния в S_i – е состояние как это показано на рис. 1 [1].

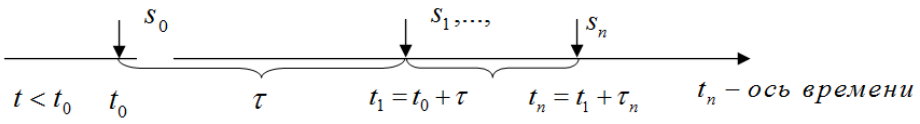

Рис. 1. Процесс перехода АИС из S_0 – го состояния в S_i – е состояние

Как видно из рис. 1 переход АИС из S_0 – го состояния в S_1 – е состояние в результате воздействия *i*-й угрозы можно представить следующим образом.

Пусть в момент времени $t < t_0$ АИС находилась в стационарном состоянии предшествующем воздействию *i*-й угрозы. Такое состояние характеризует предысторию процесса – прошлое состояние АИС до момента времени t_0. В момент времени t_0 на АИС воздействует *i*-я угроза, в результате которой АИС за время $t_1 = t_0 + \tau$ переходит из состояния S_0 – о в состояние S_1 – е. Если такой процесс соответствует Марковскому случайному процессу, то можно предсказать такой переход, учитывая только настоящее состояние АИС – S_0 и, забыв о ее предыстории. Само состояние S_0 зависит от прошлого, но, как только оно достигнуто, о прошлом состоянии можно забыть.

Таким образом, в Марковском случайном процессе будущее состояние АИС зависит от прошлого только через настоящее.

Итак, случайный процесс применительно к АИС называется Марковским, если для любого момента времени t_0 вероятностные характеристики АИС в будущем зависят только от её состояния в данный момент t_0 и не зависят от того, когда и как АИС пришла в это состояние.

Из выше сказанного следует, что для такого случайного процесса характерны [3]: случайная смена состояний АИС и вероятностная связь между предшествующими и последующими состояниями; зависимость между случайной сменой состояний АИС и временем воздействия на АИС различных угроз.

Процесс называется процессом с непрерывным временем, если моменты возможных переходов из состояния в состояние не фиксированы заранее, а не определены, случайны, т.е. переход может осуществляться в любой момент времени.

Для Марковского случайного процесса с непрерывным временем существует закономерность, что время между наступлениями того или иного события является случайным, но подчиненным определенному закону. Этот закон называется показательным, а именно [3]:

$$P(t) = 1 - e^{-\lambda t}, \quad (1)$$

где t – время воздействия угрозы на АИС; λ – интенсивность воздействия; $P(t)$ – вероятность воздействия угрозы за промежуток времени Δt (скорость наступления угрозы). Частные случаи, вытекающие из выражения (1):

если $\Delta t \to 0$, тогда $P(t) = 0$ .2; если $\Delta t \to \infty$, тогда $P(t) = 1$.

Для описания поведения такого случайного Марковского процесса используются интенсивности переходов $\lambda_{ij}(t)$, показывающие вероятность перехода системы, находящейся в состоянии i в состояние j в момент времени t, можно составить систему дифференциальных уравнений,

$$P_j(t) = \sum \lambda_{ij}(t) P_i(t),$$

решение которой определяет вероятность $P_j(t)$ нахождения системы в j-м состоянии в момент времени t.

При однородном во времени непрерывном Марковском случайном процессе условные интенсивности переходов, записываемые в виде матрицы,

$$A = \left\| \lambda_{ij} \right\|, \quad (2)$$

постоянны. Тогда система дифференциальных уравнений переходит в систему алгебраических уравнений, которую легко решить, используя преобразование Лапласа [2].

Поток событий – это последовательность однородных событий, следующих одно за другим в случайные моменты времени, например поток угроз (внутренних, внешних и др.).

Важной характеристикой потока событий является его интенсивность λ – среднее число событий в единицу времени, например, число угроз определенного класса в единицу времени. Интенсивность потока λ может быть постоянна $(\lambda = const)$ или переменна $(\lambda = var)$.

Поток событий называется регулярным, если события следуют одно за другим через равные промежутки времени.

Поток событий называется стационарным, если его вероятностные характеристики не зависят от времени.

Поток событий называется потоком без последствий, если для любых двух непересекающихся интервалов времени t_1 и t_2, число событий, попадающих на один из них, не зависит от того, сколько событий попало на другой.

Наглядной формой представления таких воздействий являются графы, с помощью которых представляются все возможные варианты событий, которые могут иметь место при воздействии на систему внешних факторов [1, 2]. Вершины графа обозначают события, а ребра – связи между ними. На каждом ребре графа можно указать соответствующую данному событию вероятность. Такой граф называется взвешенным. В теории вероятностей он носит название дерева событий или дерева возможных исходов. Граф состояний позволяет легко посчитать вероятности возможных исходов после нескольких этапов процесса.

Другой вид графа – ориентированный взвешенный граф, вершины которого обозначают не события, а состояния системы. Вершины графа соединяются стрелками, указывающими направление возможных переходов из состояния в состояние.

Если вероятности переходов связаны только с предшествующими состояниями, то реализуется процесс без последствий, или простая цепь Маркова.

Если вероятность переходов связана с учетом более ранних состояний (предыстории), то цепь Маркова называют сложной.

Если полагают, что на рассматриваемом отрезке времени переходные вероятности не зависят от номера испытания, то такая цепь Маркова называется однородной.

Цепи Маркова, в которых переходные вероятности зависят от номера испытания (различных факторов, способствующих переходу системы в различные состояния) называются неоднородными.

Переходная матрица, как правило, дополняется матрицей начального состояния. Существует два способа задания начального состояния [3]: детерминированный (неслучайный); случайный.

Такой упорядоченный набор величин (чисел) называется вектором, а сами величины или числа – компонентами вектора. Различают вектор-строку и вектор-столбец. В данном случае понятие вектора в абстрактном пространстве является пространством вероятностей.

Постановка задачи. Допущения. Граф состояния системы. Пусть на АИС за конечное время τ воздействует n простейших потоков угроз с интенсивностями λ_i, $i=1,n$ [5–8, 11, 16].

Пусть μ_i – интенсивность парирования последствий i-й угрозы. Соответственно, R_i – вероятность парирования, а $\overline{R}_i$ – вероятность не парирования i-й угрозы.

Тогда, $\mu_i \cdot R_i$ – интенсивность парирования, а $\mu_i \cdot \overline{R}_i$ – интенсивность не парирования последствий воздействия на АИС потока угроз.

Допущения:

- поток парирования и не парирования угрозы простейший;
- возможности по парированию последствий воздействия на АИС i-й угрозы не ограничены, т.е. $\mu_i \geq \lambda_i$;
- так как рассматриваются простейшие потоки, то появление одновременно двух и более угроз является невозможным событием.

Для определения вероятности благополучного исхода при воздействии на АИС потока n угроз представим систему АИС в виде графа [1, 2] (рис. 2).

В соответствии с рис. 2 можно составить матрицу интенсивностей перехода вида (3).

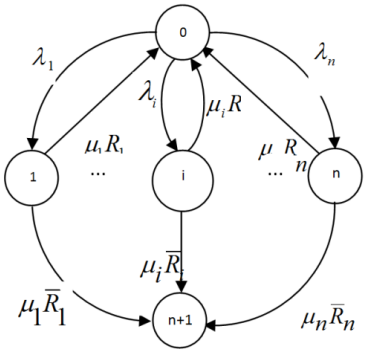

Рис. 2. Граф состояний АИС

$$\left\|\lambda_{ik}\right\| = \begin{vmatrix} -\lambda_0 & \dots & \lambda_i & \dots & \lambda_n & 0 \\ \mu_i \cdot R_i & \dots & -\mu_i & \dots & 0 & \mu_i R_i \\ \mu_n \cdot R_n & \dots & 0 & \dots & -\mu_n & \mu_n \cdot \bar{R}_n \\ 0 & \dots & 0 & \dots & 0 & \dots 0 \end{vmatrix}, \quad (3)$$

где $\lambda_0 = \lambda_1 + \lambda_2 + \dots + \lambda_n$, $j = k = 1,2,\dots,n+2$

В соответствии с рис. 2 АИС в момент времени τ может находиться в одном из следующих состояний:

- состояние «0» – поток угроз за время τ не проявился;
- состояние «1», …, i , …, n – одна из угроз проявилась;
- состояние «$n+1$» – неблагополучное поглощающее состояние, при котором угроза реализовалась.

Матрица (3) обладает следующими свойствами [3]:диагональные члены матрицы равны сумме остальных элементов данной строки, взятых с обратным знаком; сумма всех элементов каждой строки равна нулю; число нулевых строк в матрице интенсивностей переходов соответствует количеству поглощающих состояний; интенсивность перехода равна нулю при отсутствии стрелки.

Определение вероятностей перехода АИС в каждое возможное состояние. Для определения вероятностей перехода АИС в каждое возможное состояние воспользуемся системой дифференциальных уравнений Колмогорова, в соответствии с которыми можно написать [1, 2, 9, 12]

$$\begin{aligned} \frac{dP_0(\tau)}{d\tau} &= -P_0(\tau)\sum_{i=1}^{n}\lambda_i + \sum_{i=1}^{n}\mu_i R_i P_i(\tau), \\ \frac{dP_i(\tau)}{d\tau} &= \lambda_i P_0(\tau) - \mu_i P_i(\tau), \\ \frac{dP_{n+1}(\tau)}{d\tau} &= \sum_{i=1}^{n}\mu_i \bar{R}_i P_i(\tau). \end{aligned} \quad (4)$$

Применяя к системе дифференциальных уравнений (4) прямое преобразование Лапласа с учетом исходных данных $P_0(0) = 1$, $P_i(0) = P_{n+1}(0) = 0$ и с учетом того, что $\int_0^\infty P_i(\tau)e^{-S\tau}d\tau = -P_i(0) + SP_j(S)$, получим следующие выражения для определения вероятностей в соответствии с графом состояний (см. рис. 2)

$$
\begin{aligned}
-P_0(0)+SP_0(S)&=-\lambda_0 P_0(S)+\sum_{i=1}^{n}\mu_i R_i P_i(S),\\
-P_i(0)+SP_i(S)&=\lambda_i P_0(S)-\mu_i P_i(S),\\
-P_{n+1}(0)+SP_{n+1}(S)&=\sum_{i=1}^{n}\mu_i \overline{R}_i(S),
\end{aligned}
\tag{5}
$$

где $P_i(S)=\int_0^{\infty}P_i(\tau)e^{-St}d\tau$ – искомое изображение.

При начальных условиях система уравнений (5) примет вид:

$$
\begin{aligned}
(S+\lambda_0)P_0(S)&=\sum_{i=1}^{n}\mu_i R_i(S)=1,\\
-\lambda_i P_0(S)+(S+\mu_i)P_i(S)&=0,\\
-\sum_{i=1}^{n}\mu_i \overline{R}_i P_i(S)+SP_{n+1}(S)&=0.
\end{aligned}
\tag{6}
$$

По правилу Крамера искомые изображения определяются отношением:

$$P_j(S)=\frac{\Delta_j(S)}{\Delta(S)},\quad j=1,n,\tag{7}$$

где $\Delta(S)=S[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i)-\sum_{i=1}^{n}\lambda_i\mu_i R_i\prod_{l=1}^{n}(S+\mu_l)]$ – главный определитель системы; $\Delta_j(S)$ – частный определитель системы, находится из главного определителя путем замены j-го столбца коэффициентами, стоящими в правых частях уравнений (6).

Частные определители, полученные с помощью введения определителей по индукции, будут равны:

$$
\begin{aligned}
\Delta_0(S)&=S\prod_{l=1}^{n}(S+\mu_l),\\
\Delta_i(S)&=S\lambda_0\prod_{l=1}^{n}(S+\mu_l),\\
\Delta_{n+1}(S)&=\sum_{i=1}^{n}\lambda_i\mu_i R_i\prod_{l=1}^{n}(S+\mu_l)].
\end{aligned}
\tag{8}
$$

С учетом указанного и при условии, что $\rho_j(S)=\frac{\Delta_j(S)}{S}$, $\rho(S)=\frac{\Delta(S)}{S}$ система уравнений (6) примет вид:

$$
\begin{aligned}
P_0(S)&=\frac{q_0(S)}{\rho(S)}=\frac{\Delta_0(S)S}{S\Delta(S)}=\frac{\Delta_0(S)}{\Delta(S)},\\
P_i(S)&=\frac{q_i(S)}{\rho(S)}=\frac{\Delta_i(S)S}{S\Delta(S)}=\frac{\Delta_i(S)}{\Delta(S)},\\
P_{n+1}(S)&=\frac{q_{n+1}(S)}{\rho(S)}=\frac{\Delta_{n+1}(S)S}{S\Delta(S)}=\frac{\Delta_{n+1}(S)}{\Delta(S)}.
\end{aligned}
\tag{9}
$$

Окончательно с учетом (8) выражения (9) примут вид [1, 2, 14, 15, 18]:

$$P_0(S) = \frac{\prod_{l=1}^{n}(S+\mu_l)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i) - \sum_{i=1}^{n}\lambda_i\mu_i R_i \prod_{l=1}^{n}(S+\mu_l)]},$$

$$P_i(S) = \frac{\lambda_0 \prod_{l=1}^{n}(S+\mu_l)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i) - \sum_{i=1}^{n}\lambda_i\mu_i R_i \prod_{l=1}^{n}(S+\mu_l)]}, \qquad (10)$$

$$P_{n+1}(S) = \frac{\sum_{i=1}^{n}\lambda_i\mu_i R_i \prod_{l=1}^{n}(S+\mu_l)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i) - \sum_{i=1}^{n}\lambda_i\mu_i R_i \prod_{l=1}^{n}(S+\mu_l)]}.$$

Тогда из (10) следует, что вероятность благополучного исхода от воздействия на АИС n независимых потоков внутренних угроз определяется следующим выражением: $P_{БИ}(\tau) = \sum_{i=1}^{n} P_i(\tau)$, а вероятность противоположного события, т.е. неблагополучного исхода, будет равна $P_{БИ}(\tau) = 1 - \sum_{i=1}^{n} P_i(\tau) = P_{n+1}(\tau)$.

Частные случаи:

1. Интенсивность парирования i-го потока угрозы μ_i равно интенсивности воздействия i-го потока угрозы λ_i

Пусть $\mu_i = \lambda_i$, т.е. интенсивность парирования последствий i-го потока угроз равна интенсивности i-го потока угроз.

Тогда изображения вероятностей можно представить следующим образом [1, 2, 14, 15, 18]:

$$P_0(S) = \frac{\prod_{i=1}^{n}(S+\lambda_i)}{(S+\lambda_0)\prod_{i=1}^{n}(S+\lambda_i) - \sum_{i=1}^{n}\lambda_i^2 R_i \prod_{\substack{l=1 \\ l\neq i}}^{n}(S+\lambda_l)};$$

$$P_i(S) = \frac{\lambda_i \prod_{i=1}^{n}(S+\lambda_i)}{(S+\lambda_0)\prod_{i=1}^{n}(S+\lambda_i) - \sum_{i=1}^{n}\lambda_i^2 R_i \prod_{\substack{l=1 \\ l\neq i}}^{n}(S+\lambda_l)}; \qquad (11)$$

$$P_{n+1}(S) = \frac{1}{S}\sum_{i=1}^{n}\lambda_i \bar{R}_i P_i(S).$$

Функции $q_i(S)$ и $\rho(S)$ могут быть представлены в виде полиномов с коэффициентами b_i и c_i, а именно:

$$\begin{aligned} q_0(S) &= S^n + b_{n-1}S^{n-1} + ,\ldots, + b_1 S + b_0 \\ q_i(S) &= S^{n-1} + b_{n-2}S^{n-2} + ,\ldots, + b_1 S + b_0 \\ \rho(S) &= S^{n+1} + c_n S^n + ,\ldots, + c_1 S + c_0 \end{aligned} \qquad (12)$$

Из выражения (12) следует, что изображения вероятностей $P_j(S)$ являются правильными рациональными дробями, у которых степени полиномов числителей численно меньше полиномов знаменателей.

Тогда применяя к (12), табличное преобразование Лапласа, получим следующее выражение для характеристических оригиналов искомых вероятностей:

$$G^{-1}(P_j(S)) = \begin{cases} \sum_{k=1}^{\omega} \frac{1}{\rho_j'(S_k)} e^{S_k \tau}, \ \textit{если } P_j(S) = \frac{1}{\rho_i(S)}, \\ \sum_{k=1}^{\omega} \frac{q_j(S_k)}{\rho_j'(S_k)} e^{S_k \tau}, \ \textit{если } P_j(S) = \frac{q_i(S)}{\rho_j(S)}, \\ a\left[\frac{1}{\rho_j(0)} + \sum_{k=1}^{\omega} \frac{1}{S_k \rho_j'(S_k)} e^{S_k \tau}\right], \ \textit{если } P_j(S) = \frac{a}{S\rho_j(S)}. \end{cases} \quad (13)$$

где ω – количество корней *i*-го характеристического уравнения; a – константа

Тогда с учетом нормированного условия $\sum_{i=1}^{n} P_i = 1$, где P_i – вероятность нахождения АИС в *i*-м состоянии, можно записать, что конечная вероятность

$$P_{БИ}(\tau) = \sum_{i=0}^{n} P_j(\tau) \quad (14)$$

характеризует благополучный исход, а

$$Q_{БИ}(\tau) = 1 - \sum_{j=0}^{n} P_j(\tau) = P_{n+1}(\tau) \quad (15)$$

неблагополучный исход от воздействия на АИС различных угроз.

2. Оценки вероятностей последствий от реализации угроз безопасности ИОР с учетом воздействия на АИС одного потока угроз. Для практических расчетов наиболее часто имеет место случай, когда на АИС воздействует один поток угроз, т.е. $n = 1$.

Пусть на АИС, в течении времени τ, воздействует один поток угроз с интенсивностью – λ, интенсивность парирования – μ и вероятность парирования потока угроз – R.

Тогда из системы уравнений (13) при $n = 1$ изображения вероятностей примут следующий вид [1, 2, 18]:

$$\begin{aligned} P_0(S) &= \frac{S + \mu}{(S + \lambda)(S + \mu) - \lambda\mu R} = \frac{q_0(S)}{\rho(S)}, \\ P_1(S) &= \frac{\lambda}{(S + \lambda)(S + \mu) - \lambda\mu R} = \frac{q_1(S)}{\rho(S)}, \\ P_{n+1}(S) &= \frac{\lambda\mu\bar{R}}{S[(S + \lambda)(S + \mu) - \lambda\mu R]} = \frac{q_{n+1}(S)}{S\rho(S)}, \end{aligned} \quad (16)$$

где $\rho(S) = S^2 + Sc_1 + c_0$, $c_1 = \lambda + \mu$, $c_0 = \lambda\mu\bar{R}$.

Применяя к (16) обратное преобразование Лапласа с учетом (14) и (15) получим выражения для определения искомых вероятностей, а именно:

$$P_0(\tau) \to P_0(\tau) = \frac{1}{2\sqrt{\Lambda}} e^{-\frac{c_1}{2}\tau} [(\mu - \lambda - \Lambda) e^{-\frac{\sqrt{\Lambda}}{2}\tau} - (\mu - \lambda - \sqrt{\Lambda} e^{-\frac{\sqrt{\Lambda}}{2}\tau})]; \quad (17)$$

$$P_1(\tau)=\frac{\lambda}{\sqrt{\Lambda}}e^{-\frac{c_1}{2}\tau}[e^{-\frac{\sqrt{\Lambda}}{2}\tau}-e^{-\frac{\sqrt{\Lambda}}{2}\tau})]; \quad (18)$$

$$P_{n+1}(\tau)=1-\frac{2\lambda\mu\bar{R}}{\sqrt{\Lambda}}e^{-\frac{c_1}{2}\tau}[\frac{1}{\lambda+\mu-\sqrt{\Lambda}}e^{-\frac{\sqrt{\Lambda}}{2}\tau}-\frac{1}{\lambda+\mu+\sqrt{\Lambda}}e^{-\frac{\sqrt{\Lambda}}{2}\tau})]; \quad (19)$$

где $\Lambda=c_1^2-4c_0=\lambda^2+2\lambda\mu(1-2\bar{R})+\mu^2.$

Тогда с учетом (14) и (15) вероятность благополучного исхода от воздействия на АИС одного потока угроз будет равна

$$P_{БИ}(\tau)=P_0(\tau)+P_1(\tau), \quad (20)$$

а вероятность неблагополучного исхода

$$Q_{БИ}(\tau)=P_{n+1}(\tau) \quad (21)$$

Случай, когда $\lambda=\mu$. Тогда выражения (17), (18), (19) будут иметь вид:

$$P_0(\tau)=\frac{1}{2}e^{-\lambda t}[e^{\lambda\sqrt{R}\tau}+e^{-\lambda\sqrt{R}\tau}], \quad (22)$$

$$P_1(\tau)=\frac{1}{2\sqrt{R}}e^{-\lambda t}[e^{\lambda\sqrt{R}\tau}-e^{-\lambda\sqrt{R}\tau}], \quad (23)$$

$$P_{n+1}(\tau)=1-\frac{\bar{R}}{2\sqrt{R}}e^{-\lambda t}[\frac{1}{1-\sqrt{R}}e^{\lambda\sqrt{R}\tau}-\frac{1}{1+\sqrt{R}}e^{-\lambda\sqrt{R}\tau}]. \quad (24)$$

Конечные вероятности (17), (18) и (19) определяются, используя выражения (22), (23) и (24).

Учитывая переходные интенсивности для матрицы (3), система дифференциальных уравнений имеет следующий вид:

$$\begin{aligned}
\frac{dP_0(\tau)}{d\tau}&=-\lambda_{00}P_0(\tau)+\mu_1R_1P_1(\tau)+\mu_2R_2P_2(\tau)\\
\frac{dP_1(\tau)}{d\tau}&=\lambda_{01}P_0(\tau)-\mu_1P_1(\tau)+\mu_2r_{12}P_2(\tau),\\
\frac{dP_2(\tau)}{d\tau}&=\lambda_{02}P_0(\tau)+\mu_1r_{12}P_1(\tau)-\mu_2P_2(\tau),\\
\frac{dP_3(\tau)}{d\tau}&=\mu_1\bar{R}_{13}P_1(\tau)+\mu_2R_{23}P_2(\tau).
\end{aligned} \quad (25)$$

Применяя к системе дифференциальных уравнений (25) принятое преобразование Лапласа с учетом исходных данных $P_0(0)=1$, $P_1(0)=P_2(0)=P_3(0)=0$ представляется возможным получить выражения для определения вероятностей $P_0(\tau)$, $P_1(\tau)$, $P_2(\tau)$, $P_3(\tau)$.

Выводы.

1. Обоснована применимость Марковских случайных процессов для оценки влияния различных угроз на безопасность конфиденциальной информации. Дано понятие Марковского случайного процесса с учетом воздействия на АИС различных угроз. Показано, что Марковские случайные процессы могут быть использованы для оценки вероятности благополучного или неблагополучного исхода при воздействии на АИС угроз. Для определения указанных вероятностей целесообразно представить последовательность переходов АИС из одного *i*-го состояния в другое *j*-е в виде графа состояний, который называется цепью Маркова.

2. Разработаны математические методы исследования безопасности КИ на основе Марковского случайного процесса с непрерывным параметром. Показано, что в Марковском случайном процессе с непрерывным параметром переходы АИС из одного состояние в другое задаются интенсивностями переходов. На основе графа состояний составлена матрица интенсивностей переходов, а также система дифференциальных уравнений Колмогорова, решение которых с учетом прямого преобразования Лапласа позволяет получить вероятности нахождения системы в соответствующих состояниях и вероятность благополучного исхода от воздействия на АИС независимых и зависимых потоков угроз.

3. На основе указанного подхода разработаны математические методы с учетом воздействия на АИС n независимых потоков угроз, а также когда интенсивность парирования i-го потока угрозы μ_i равно интенсивности воздействия i-го потока угрозы λ_i и одной i-й угрозы (как частные случаи).

4. Предложенные методы и методики на основе МСП показали возможность количественной оценки безопасности ИОР, что позволит, используя полученные данные, разрабатывать научно-обоснованные организационно-профилактических мероприятий по повышению уровня защищенности информации ограниченного распространения, циркулирующей в различных структурных образованиях РФ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Росенко А.П.* Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации: Монография. – М.: Гелиос АРВ, 2008. – 154 с.
2. *Росенко А.П.* Внутренние угрозы безопасности конфиденциальной информации: методология и теоретическое исследование: Монография. – М.: КРАСАНД, 2010. – 160 с.
3. *Тихонов В.И., Миронов М.А.* Марковские процессы. – М.: Советское радио, 1997. – 488 с.
4. *Росенко А.П.* Методологические основы проблемы безопасности конфиденциальной информации // Известия ТРТУ. – 2006. – № 7 (62). – С. 27-33.
5. *Росенко А.П.* Применение Марковских случайных процессов с дискретным параметром для оценки уровня информационной безопасности // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 169-172.
6. *Росенко А.П.* Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 71-81.
7. *Росенко А.П.* Об одном подходе к определению вероятностей последствий от воздействия на АИС угроз безопасности конфиденциальной информации // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 164-168.
8. *Росенко А.П., Клименко Е.С.* Математическое моделирование безопасности конфиденциальной информации с учетом воздействия на автоматизированную информационную систему зависимых внутренних угроз // Научно-технические ведомости СПб ГПУ. Информатика. Телекоммуникации. Управление. – St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control Systems. – 2009. – Т. 6, № 91. – С. 93-99.
9. *Росенко А.П.* О критерии нормирования уровня безопасности конфиденциальной информации // Обозрение прикладной и промышленной математики. – М.: Изд-во «ОП и ПМ», 2010. Т. 17 (2). Научные доклады. Ч. 1. – С. 297-298.
10. *Росенко А.П., Лоба И.С.* К вопросу применения Марковских случайных процессов с непрерывным параметром для оценки влияния внутренних угроз на безопасность конфиденциальной информации // Материалы 9-й Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2007. – С. 60-64.
11. *Росенко А.П.* Методы определения вероятности несанкционированного доступа к конфиденциальной информации // Доклады Томского гос. ун-та систем управления и радиоэлектроники. – 2012. – № 1–2. – С. 25-28.
12. *Росенко А.П.* Методика обработки массива исходных данных, полученных экспертным путем // Доклады Томского гос. ун-та систем управления и радиоэлектроники. – 2012. – № 1–2. – С. 192-197.

13. *Росенко А.П., Клименко Е.С.* Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе// Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 71-81.
14. *Росенко А.П., Клименко Е.С.* Марковская модель оценки влияния внутренних угроз на безопасность конфиденциальной информации // Известия ТРТУ. – 2007. – № 1 (76). – С. 123-126.
15. *Росенко А. П., Окулов Н.С.* Программа расчета количественной оценки безопасности информации ограниченного распространения // Свидетельство о государственной регистрации программ для ЭВМ № 2015619521, зарегистрированное в Реестре программ для ЭВМ от 04 сентября 2015 г.
16. *Росенко А.П. Бордак И.В., Зданович С.В.* Математическая модель оценки безопасности конфиденциальной информации, циркулирующей в автоматизированной информационной системе // Производственные, инновационные и информационные проблемы развития региона: сборник материалов Международной научно-практической конференции. – Ставрополь: АГРУС Ставропольского гос. Аграрного ун-та, 2014. – С. 213-216
17. К вопросу количественной оценки безопасности информации ограниченного распространения, циркулирующей в автоматизированной информационной системе военного назначения // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: сб. трудов VIII–IX Всерос. НТК. г. Геленджик 2014 г. – Краснодар: ФВАС, 2014. – 480 с.
18. *Росенко А.П., Бордак И.В.* Метод определения вероятности несанкционированного доступа злоумышленника к конфиденциальной информации // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: сб. трудов VIII–IX Всерос. НТК. г. Геленджик 2014 г. – Краснодар: ФВАС, 2014. – 480 с.
19. *Росенко А.П.* Анализ и обобщение существующих подходов к классификации угроз безопасности конфиденциальной информации // Вестник Северо-Кавказского федерального университета. – 2013. – № 3 (36). – С. 30-34.

REFERENCES

1. *Rosenko A.P.* Teoreticheskie osnovy analiza i otsenki vliyaniya vnutrennikh ugroz na bezopasnost' konfidentsial'noy informatsii: Monografiya [Theoretical framework for the analysis and evaluation of the influence of internal threats on the security of confidential information: a Monograph]. Moscow: Gelios ARV, 2008, 154 p.
2. *Rosenko A.P.* Vnutrennie ugrozy bezopasnosti konfidentsial'noy informatsii: metodologiya i teoreticheskoe issledovanie: Monografiya [Internal threats to the security of confidential information: methodology and theoretical research: Monograph]. Moscow: KRASAND, 2010, 160 p.
3. *Tikhonov V.I., Mironov M.A.* Markovskie protsessy [Markov processes]. Moscow: Sovetskoe radio, 1997, 488 p.
4. *Rosenko A.P.* Metodologicheskie osnovy problemy bezopasnosti konfidentsial'noy informatsii [Methodological basis of the problem of security of confidential information], *Izvestiya TRTU* [Izvestiya TSURe], 2006, No. 7 (62), pp. 27-33.
5. *Rosenko A.P.* Primenenie Markovskikh sluchaynykh protsessov s diskretnym parametrom dlya otsenki urovnya informatsionnoy bezopasnosti [Application of Markov random process with discrete parameters for assessing of information security level], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11 (100), pp. 169-172.
6. *Rosenko A.P.* Matematicheskoe modelirovanie vliyaniya vnutrennikh ugroz na bezopasnost' konfidentsial'noy informatsii, tsirkuliruyushchey v avtomatizirovannoy informatsionnoy sisteme [Mathematical modeling of internal threats on safety of the confidential information circulating in automated information system availability], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 8 (85), pp. 71-81.
7. *Rosenko A.P.* Ob odnom podkhode k opredeleniyu veroyatnostey posledstviy ot vozdeystviya na AIS ugroz bezopasnosti konfidentsial'noy informatsii [One approach to determining consequences probabilities of exposure to AIS information security threats], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11 (100), pp. 164-168.

8. *Rosenko A.P., Klimenko E.S.* Matematicheskoe modelirovanie bezopasnosti konfiden-tsial'noy informatsii s uchetom vozdeystviya na avtomatizirovannuyu informatsionnuyu sistemu zavisimykh vnutrennikh ugroz [Mathematical modeling the security of confidential information taking into account the impact on automated information system of dependent internal threats], *Nauchno-tekhnicheskie vedomosti SPb GPU. Informatika. Telekommunikatsii. Upravlenie* [Scientific and technical Gazette of St. Petersburg GPU. Informatics. Telecommunications. Management]. St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control Systems, 2009, Vol. 6, No. 91, pp. 93-99.
9. *Rosenko A.P.* O kriterii normirovaniya urovnya bezopasnosti konfidentsial'noy informatsii [About criteria of rating of level of security of confidential information], *Obozrenie prikladnoy i promyshlennoy matematiki* [Review of applied and industrial mathematics]. Moscow: Izd-vo «OP i PM», 2010. Vol. 17 (2). Nauchnye doklady. Part 1, pp. 297-298.
10. *Rosenko A.P., Loba I.S.* K voprosu primeneniya Markovskikh sluchaynykh protsessov s nepreryvnym parametrom dlya otsenki vliyaniya vnutrennikh ugroz na bezopasnost' kon-fidentsial'noy informatsii [To the use of Markov processes with continuous parameter to assess the impact of internal threats to the security of confidential information], *Materialy 9-y Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'»* [Proceed-ings of 9-th International scientific-practical conference "Information security"]. Part 1. Taganrog: Izd-vo TTI YuFU, 2007, pp. 60-64.
11. *Rosenko A.P.* Metody opredeleniya veroyatnosti nesanktsionirovannogo dostupa k kon-fidentsial'noy informatsii [Metody opredeleniya veroyatnosti nesanktsionirovannogo dostupa k konfidentsial'noy informatsii], *Doklady Tomskogo gos. un-ta sistem upravleniya i radioelektroniki* [Reports of Tomsk state University of control systems and Radioelectronics], 2012, No. 1–2, pp. 25-28.
12. *Rosenko A.P.* Metodika obrabotki massiva iskhodnykh dannykh, poluchennykh ekspertnym putem [The method of processing the source data obtained by the expert], *Doklady Tomskogo gos. un-ta sistem upravleniya i radioelektroniki* [Reports of Tomsk state University of control systems and Radioelectronics], 2012, No. 1–2, pp. 192-197.
13. *Rosenko A.P., Klimenko E.S.* Matematicheskoe modelirovanie vliyaniya vnutrennikh ugroz na bezopasnost' konfidentsial'noy informatsii, tsirkuliruyushchey v avtomatizirovannoy informatsionnoy sisteme [Mathematical modeling of internal threats on safety of the confiden-tial information circulating in automated information system availability], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 8 (85), pp. 71-81.
14. *Rosenko A.P., Klimenko E.S.* Markovskaya model' otsenki vliyaniya vnutrennikh ugroz na bezopasnost' konfidentsial'noy informatsii [A Markov model for assessing the impact of external threats on the security of confidential information], *Izvestiya TRTU* [Izvestiya TSURe], 2007, No. 1 (76), pp. 123-126.
15. *Rosenko A. P., Okulov N.S.* Programma rascheta kolichestvennoy otsenki bezopasnosti informatsii ogranichennogo rasprostraneniya [The program of calculation of the quantitative safety assess-ment of restricted information], *Svidetel'stvo o gosudarstvennoy registratsii programm dlya EVM № 2015619521, zaregistrirovannoe v Reestre programm dlya EVM ot 04 sentyabrya 2015 g* [The certificate of state registration of computer programs No. 2015619521 registered in the Regis-try of the computer programs from 04 September 2015].
16. *Rosenko A.P. Bordak I.V., Zdanovich S.V.* Matematicheskaya model' otsenki bezopasnosti konfidentsial'noy informatsii, tsirkuliruyushchey v avtomatizirovannoy informatsionnoy sisteme [A mathematical model to assess the security of confidential information circulating in the au-tomated information system], *Proizvodstvennye, innovatsionnye i informatsionnye problemy razvitiya regiona: sbornik materialov Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Pro-duction, innovation and information problems of development of the region: collection of ma-terials of International scientific-practical conference]. Stavropol': AGRUS Stavropol'skogo gos. Agrarnogo un-ta, 2014, pp. 213-216.
17. K voprosu kolichestvennoy otsenki bezopasnosti informatsii ogranichennogo rasprostraneniya, tsirkuliruyushchey v avtomatizirovannoy informatsionnoy sisteme voennogo naznacheniya [To the question of quantitative evaluation of security of information limited the spread of circulating in the au-tomated information system for military use], *Informatsionnaya bezopasnost' – aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nykh tekhnologiy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti: sb. trudov VIII–IX Vseros. NTK. g. Gelendzhik 2014 g.* [Information se-curity is a current problem. Improvement of educational technologies of training specialists in the field of information security: collection of works the VIII–IX All-Russian the scientific and technical con-ferencing. Gelendzhik 2014]. Krasnodar: FVAS, 2014, 480 p.

18. *Rosenko A.P., Bordak I.V.* Metod opredeleniya veroyatnosti nesanktsionirovannogo dos-tupa zloumyshlennika k konfidentsial'noy informatsii // Informatsionnaya bezopasnost' – aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nykh tekhnologiy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti: sb. trudov VIII–IX Vseros. NTK. g. Gelendzhik 2014 g. [*Informatsionnaya bezopasnost' – aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nykh tekhnologiy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti: sb. trudov VIII–IX Vseros. NTK. g. Gelendzhik 2014 g.* [Information security is a current problem. Improvement of educational technologies of training specialists in the field of information security: collection of works the VIII–IX All-Russian the scientific and technical conferencing. Gelendzhik 2014]. Krasnodar: FVAS, 2014, 480 p.
19. *Rosenko A.P.* Analiz i obobshchenie sushchestvuyushchikh podkhodov k klassifikatsii ugroz bezopasnosti konfidentsial'noy informatsii [Analysis and synthesis of existing approaches to the classification of threats to the security of confidential information] *Vestnik Severo-Kavkazskogo federal'nogo universiteta* [Vestnik of North-Caucasus Federal University], 2013, No. 3 (36), pp. 30-34.

Статью рекомендовал к опубликованию д.т.н., профессор В.Д. Ковалев.

Росенко Александр Петрович – ФГАОУ ВПО «Северо-Кавказский федеральный университет»; e-mail: rap.44@mail.ru, 355009, г. Ставрополь, ул. Беличенко, 2, кв. 21; тел.: 89197506556, кафедра прикладной математики и компьютерной безопасности; доцент.

Бордак Ирина Владимировна – e-mail: irinabordak@mail.ru; 355005, г. Ставрополь, ул. Гофицкого, 107г; тел.: 89188777404, кафедра прикладной математики и компьютерной безопасности; аспирант.

Rosenko Alexander Petrovich – FGAOU VPO "North-Caucasian Federaltion University"; e-mail: rap.44@mail.ru; 355009, Stavropol, St. Belichenko, 2, sq. 21; phone: +79197506556, the department of applied mathematics and computer security; associate professor.

Bordak Irina Vladimirovna – e-mail: irinabordak@mail.ru, 355005, Stavropol, St. Gorickogo, 107g; phone: +79188777404; the department of applied mathematics and computer security; post-graduate student.

УДК 004.67

П.С. Поперечный

РАЗРАБОТКА ПАРАЛЛЕЛЬНОГО КОДЕРА БЧХ С РЕГУЛИРУЕМОЙ КОРРЕКТИРУЮЩЕЙ СПОСОБНОСТЬЮ

Целью данной статьи является описание способа распараллеливания кодера БЧХ (Боуза–Чоудхури–Хоквингема) с возможностью изменять корректирующую способность кода. Представлена схема традиционного кодера, но с реконфигурируемым порождающим полиномом, хранящимся в перезаписываемых регистрах. Также предложена схема распараллеливания кодера в общем виде для любой ширины шины данных. В результате предложена схема параллельного реконфигурируемого кодера в общем виде для любой шины данных и любого полинома. Выведено аналитическое выражение для параллельной реализации кодера, с переменным количеством исправляемых ошибок. Данное выражение позволяет выполнить как программную, так и аппаратную реализацию кодера. Аппаратно реализовано устройство кодирования предложенным способом. Приведено подробное описание устройства, а также произведено сравнение с аналогичными устройствами с различной шириной входной шины данных с помощью современных САПР на базе ПЛИС. Показано, что за счет своей универсальности в применении для различных накопителей, разработанное устройство имеет преимущество по аппаратным ресурсам. Так же ввиду параллельной обработки входных данных устройство обладает большей пропускной способностью в сравнении с традиционным кодером. Такой подход распараллеливания может применяться при разработке устройств кодирования в системах на кристалле, в контроллерах памяти,