конечно, при условии, что $1 - \lambda_0\beta > 0$.

Сделав определенные предположения о характеристиках потока отказов системы обработки сообщений, проектировщик может по формуле (8) определить необходимое значение среднего времени обработки сообщений, которое обеспечит заданные средние временные характеристики процесса обработки данных с учетом ненадежной работы системы.

Выводы

1. Формально поставлена и решена задача определения интенсивности обработки сообщения, гарантирующей выполнение заданных ограничений на среднее время задержек обработки запросов в системе. Получено точное решение для системы **M/G/1** и приближенное решение для системы **G/G/1**. Предложен вариант решения задачи для системы $\mathbf{M_n/G_n/1}$ с бесприоритетной дисциплиной обслуживания и системой относительных приоритетов.

2. Формально поставлена и решена задача учета влияния предположения о ненадежной работе оборудования на определение интенсивности обработки сообщений, гарантирующей выполнение заданных ограничений на среднее время задержек обработки запросов в системе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Башарин Г.П., Бочаров П.П., Коган Я.А.* Анализ очередей в вычислительных сетях. Теория и методы расчета. – М.: Наука, 1989. – 336 с.

2. *Клейнрок Л.* Вычислительные системы с очередями – М.: Мир, 1979. – 600 с.

3. *Смирнов С.Н.* Метод проектирования систем с заданными задержками обслуживания. // Вестник Российского университета дружбы народов. Серия “Прикладная и компьютерная математика”. – М.: Изд-во Российского университета дружбы народов, 2003. Т.2. – № 1. – С. 52-67.

4. *Cohen J.W.* The single-server queue. – NY: Prentice-Hall, 1969. – 736 p.

УДК 004.942

А.П. Росенко

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВЛИЯНИЯ ВНУТРЕННИХ УГРОЗ НА БЕЗОПАСНОСТЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ*

1. Актуальность проблемы

Известно, что аппарат теории марковских случайных процессов широко используется при исследовании поведения различных технических систем [1,2]. В [3] показано, что марковские случайные процессы могут быть использованы и для оценки влияния внутренних угроз на безопасность конфиденциальной информации. Актуальность указанной проблемы связана с тем, что, как показывает анализ [4,5], от 65 до 85% всех реализованных угроз обусловлено внутренними угрозами. Однако отсутствие системных исследований в этой области существенно усложняет процедуру установления причинно-следственных связей, возникающих в человеко-машинной информационной системе в процессе воздействия на нее дестабилизирующих факторов различной природы [3,4]. Это связано с тем, что после воздействия на автоматизированную информационную систему (АИС) внутренних

* Работа выполнена при поддержке гранта РФФИ № 06-01-00020а.

угроз она переходит в новое, отличное от исходного, состояние. При этом, переход системы в конечное поглощающее состояние может быть с последствиями (неблагополучный исход) или без последствий (благополучный исход). Указанные особенности, а также то, что реализации внутренних угроз являются редкими, независимыми событиями, позволяют предположить, что для исследования влияния внутренних угроз на безопасность конфиденциальной информации оправдано применение теории марковских случайных процессов [3].

2. Общая постановка задачи

Предположим, что АИС может находиться в n - возможных случайных состояниях $x_1, x_2, ..., x_n$. Состояние перехода АИС из i-го в j-е состояние тоже является случайным и характеризуется вероятностью P_{ij}. Если для каждого состояния известны вероятности перехода АИС в любое другое состояние, то можно составить матрицу переходных вероятностей вида:

$$\left\| P_{ij} \right\| = \begin{vmatrix} P_{11} & P_{12} & \dots & P_{ij} & \dots & P_{1n} \\ P_{21} & P_{22} & \dots & P_{2j} & \dots & P_{2n} \\ . & . & . & . & . & . \\ P_{i1} & P_{i2} & \dots & P_{ij} & \dots & P_{in} \\ . & . & . & . & . & . \\ P_{n1} & P_{n2} & \dots & P_{nj} & \dots & P_{nn} \end{vmatrix}. \quad (1)$$

Пусть в начальный момент (перед первым шагом) АИС находится в состоянии x_n. Тогда, для начального момента $(n=0)$ вероятности всех состояний равны нулю, кроме вероятности начального состояния $P_n(0)=1$. После первого шага $(k=1)$ АИС перейдет из состояния x_n в одно из состояний $x_1, x_2, ..., x_n, ..., x_k$ с вероятностями: $P_{n1}, P_{n2}, ..., P_{nn}, ..., P_{nk}$. Тогда n-я строчка матрицы переходных вероятностей будет иметь вид

$$P_1(1) = P_{n1};\ P_2(1) = P_{n2} \dots,\ P_n(1) = P_{nn}, \dots,\ P_k(1) = P(nk) \quad (2)$$

Вероятности состояний после второго шага определяются по формуле полной вероятности[2]. Тогда

$$P_i(2) = \sum_{j=1}^{3} P_j(1) \cdot P_{ij}\ . \quad (3)$$

При этом должна выполняться гипотеза о том, что АИС после первого шага может быть в любом из возможных состояний. Тогда с учетом (2) и в соответствии с (3) по формуле полной вероятности матрица переходных вероятностей после k-го шага будет иметь вид

$$P_i(k) = \sum_{j=1}^{k} P_j(k-1) P_{ji}\ , \quad (4)$$

где $i = 1,2,...,k$;

а вероятности перехода АИС из i-го в j-е состояние за k шагов

$$P_{ij} = \sum_{n=1}^{k} P_{in} P_{nj} (k-1), \qquad (5)$$

где $k \geq 2$.

Решение системы уравнений (4) позволяет определить любую вероятность $P_i(k)$ при известных начальных условиях: $P_1(0), P_2(0), ..., P_k(0)$, т.е. при известном начальном состоянии системы. Исходными данными в этом случае служат вероятности перехода, которые могут задаваться стохастической матрицей вида (1).

3. Постановка задачи с учётом воздействия на АИС внутренних угроз

Пусть на АИС воздействует n независимых внутренних угроз. При этом очередная внутренняя угроза воздействует на систему только после успешного парирования предыдущей. Процесс перехода системы из состояния в состояние происходит до тех пор, пока она не окажется в поглощающем состоянии, соответствующего реализации злоумышленником внутренних угроз.

Примем следующие обозначения: R_i и $\overline{R}_i = 1 - R_i$ – вероятности соответственно успешного и неуспешного парирования возникшей i-й внутренней угрозы; q_i и $P_i = 1 - q_i$ – вероятности соответственно возникновения и не возникновения i-й внутренней угрозы; $0,1,...,i,...,n,n+1$ – состояния, в которых может оказаться рассматриваемая система в результате воздействия n независимых внутренних угроз. При этом, состояние $n+1$ соответствует поглощающему состоянию.

Для указанного выше случая граф состояний представлен на рис. 1.

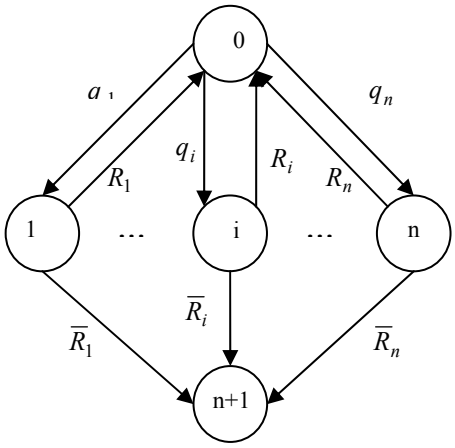

Рис. 1. Граф состояния системы при воздействии на нее n независимых внутренних угроз

Как видно из рис. 1, при любом i-м воздействии система может оказаться с вероятностью R_i в исходном состоянии, что соответствует успешному парированию i-й внутренней угрозы, и с вероятностью $\overline{R}_i = 1 - R_i$ в поглощающем состоянии $n+1$, что соответствует реализации злоумышленником i-й внутренней угрозы.

В соответствии с рис. 1 матрица переходных вероятностей будет иметь следующий вид:

$$\left\|P_{ij}\right\| = \begin{vmatrix} q_{00} & q_1 & \dots & q_i & \dots & q_n & 0 \\ R_1 & q_{11} & \dots & 0 & \dots & 0 & \overline{R}_1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ R_n & 0 & \dots & 0 & \dots & q_{nn} & \overline{R}_n \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{vmatrix}, \quad (6)$$

где $q_{00} = 1 - q_{\sum}$.

Определим вероятность перехода системы в любое i-е состояние для следующих исходных данных: $P_0(0) = 1$ и $P_1(0) = \dots = P_i(0) = \dots = P_n(0) = P_{n+1}(0) = 0$.

Тогда в соответствии с (2) после первого шага вероятности состояний будут иметь вид: $P_0(1) = 1 - q_{\sum}$, $P_{n+1}(0) = 0$, $P_1(1) = q_1$, …, $P_i(1) = q_i$, …, $P_n(1) = q_n$.

Можно показать, что поступая аналогичным образом с учетом произведенных преобразований вероятности после второго шага будут иметь вид:

$$P_0(2) = (1 - q_{\sum})^2 + \sum_{i=1}^{n} q_i R_i ; \quad P_1(2) = (1 - q_{\sum}) q_1 ;$$

$$\dots, \; P_i(2) = (1 - q_{\sum}) q_i ; \; \dots,$$

$$P_n(2) = (1 - q_{\sum}) q_n ; \; P_{n+1}(2) = \sum_{i=1}^{n} q_i \overline{R}_i .$$

Таким образом, уже после второго шага система может оказаться в поглощающем состоянии, т.е. в состоянии, когда злоумышленником получен доступ к конфиденциальной информации.

4. Воздействие на АИС одной независимой внутренней угрозы

Пусть на автоматизированную информационную систему воздействует одна i-я внутренняя угроза, тогда граф состояния системы, представленный на рис. 1, примет следующий вид (рис.2).

В соответствии с рис. 2 в результате воздействия внутренних угроз система может перейти в следующие состояния: состояние «0» – внутренняя угроза не проявилась; состояние «1» – внутренняя угроза с вероятностью q проявилась, при этом из этого состояния система с вероятностью R может перейти в исходное нулевое состояние, либо с вероятностью $\overline{R}$ в состояние «2»; состояние «2» – поглощающее состояние, т.е. неблагополучный исход от воздействия на систему внутренних угроз.

Графу состояний системы, представленному на рис. 3, соответствует следующая матрица вероятностей перехода:

$$\left\|P_{ij}\right\| = \begin{vmatrix} 1-q & q & 0 \\ R & 0 & \overline{R} \\ 0 & 0 & 1 \end{vmatrix}. \quad (7)$$

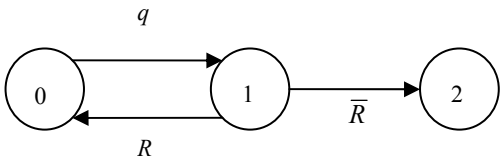

Рис. 2. Граф состояния автоматизированной информационной системы при воздействии на нее одной внутренней угрозы

Используя рис. 3 и матрицу (7) определим вероятности переходов системы в различные состояния после каждого этапа расчета для исходных данных, характеризующих вероятности состояний в начальный момент, а именно:

$$P_0(0) = 1,\ P_1(0) = P_2(0) = 0.$$

В соответствии с (4), после первого шага имеем

$$P_0(1) = 1 - q;\ P_1(1) = q;\ \ P_2(1) = 0. \qquad (8)$$

Как видно из выражения (8), после первого шага сохраняется конфиденциальность информации. После второго шага вероятности состояний системы будут иметь вид

$$P_0(2) = (1-q)^2 + qR;\ P_1(2) = (1-q)q;\ P_2(2) = q\overline{R}. \qquad (9)$$

Как видно из (9), после второго шага вероятность благополучного исхода равна $P_{БИ}(2) = P_0(2) + P_1(2) = (1-q)^2 + qP + (1-q)q$, а вероятность неблагополучного исхода от воздействия на систему одной угрозы равна $Q_{БИ}(2) = q\overline{R}$.

Пример расчета. Определим вероятность благополучного исхода от воздействия на АИС одной i-й внутренней угрозы в соответствии с рис. 3.

Исходные данные для расчета: матрица вероятностей перехода (7); $P_0(0) = 1$; $P_1(0) = 0$; $P_2(0) = 0$; количество шагов моделирования $k = 12$; в качестве внутренней угрозы воздействующей на АИС примем кражу конфиденциальной информации с электронных носителей, вероятность реализации которой $q_{BY} = 0{,}658$ [6], тогда вероятность $p_{BY} = 1 - q_{BY} = 0{,}342$; вероятность парирования внутренних угроз варьируется в пределах от $R_1 = 0{,}2$ до $R_4 = 0{,}8$.

Результаты моделирования указанного случая представлены на рис. 3.

Анализ результатов моделирования (рис. 3), позволяет сделать следующие выводы:

- после первого шага моделирования система не переходит в поглощающее состояние, что соответствует благополучному исходу от воздействия на АИС внутренней угрозы;
- начиная со второго шага моделирования, система с определенной вероятностью может попасть в поглощающее состояние. При этом вероятность такого состояния существенно зависит от возможностей собственника конфиденциальной информации по парированию проявившейся внутренней угрозы, например, как

видно из рис. 3, после пятого шага при $R_1 = 0,2$ вероятность благополучного исхода $P = 0,8$, а при $R_4 = 0,8$ вероятность $P = 0,68$;

- абсолютная величина вероятности перехода системы в поглощающее состояние возрастает с увеличением количества шагов моделирования, что свидетельствует о необходимости применения собственником конфиденциальной информации более надежных и совершенных защитных механизмов в случае многократного проявления и реализации злоумышленником внутренних угроз.

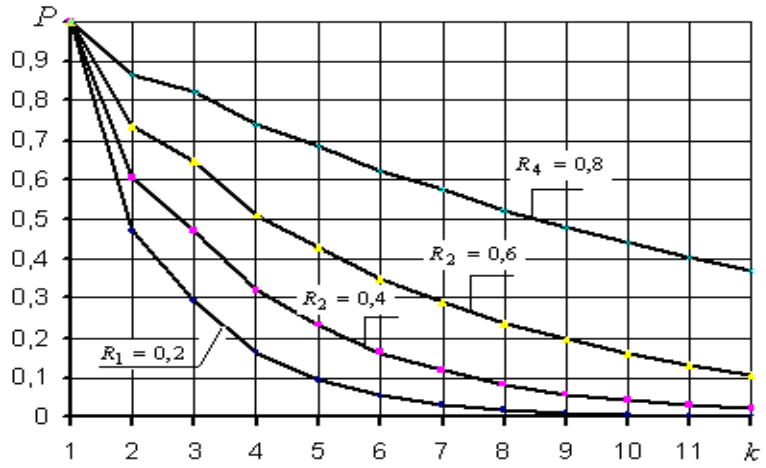

Рис. 3. Результаты моделирования воздействия на АИС одной внутренней угрозы

5. Воздействие на АИС двух зависимых внутренних угроз

Пусть на систему воздействуют две зависимые внутренние угрозы, как это показано на рис. 4, которые могут взаимно порождаться с вероятностями, соответственно, r_{12} и r_{21}.

Обозначим через q_1 и q_2 соответственно вероятность возникновения первой и второй угрозы (рис. 4).

Парирование первой и второй внутренних угроз происходит с вероятностью R_1 и R_2, а вероятности непарирования соответственно $\overline{R}_{13}$ и $\overline{R}_{23}$.

В соответствие с рис.4 система может находиться в следующих состояниях: состояние «0» – внутренние угрозы не проявляются; состояние «1» – первая внутренняя угроза проявляется с вероятностью q_1, ее парирование осуществляется с вероятностью R_1, что соответствует переходу АИС из состояния «1» в исходное, нулевое состояние; состояние «2» – вторая внутренняя угроза проявляется с вероятностью q_2, ее парирование и переход в нулевое состояние осуществляется с вероятностью R_2; состояние «3» – поглощающее состояние. В это состояние система может перейти из состояния «1» с вероятностью $\overline{R}_{13}$ и из состояния «2» с вероятностью $\overline{R}_{23}$. Поглощающее состояние соответствует реализации злоумышленником внутренних угроз.

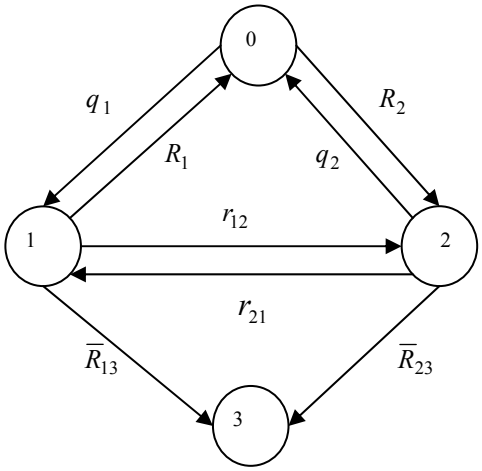

Рис. 4. Граф состояний при воздействии на систему двух независимых внутренних угроз

Как видно из рис. 4, система может находиться в состоянии «1» без парирования второй внутренней угрозы, и, наоборот, в состоянии «2» без парирования первой внутренней угрозы. Это возможно, когда первая внутренняя угроза возникает независимо от второй, но порождает ее либо, когда вторая внутренняя угроза возникает независимо от первой.

В соответствии с рис. 4, матрицу вероятностей перехода системы из состояния в состояние можно представить следующим образом:

$$\left\| P_{ij} \right\| = \begin{vmatrix} 1-q_{\sum} & q_1 & q_2 & 0 \\ R_1 & 0 & r_{12} & \overline{R}_{13} \\ R_2 & r_{21} & 0 & \overline{R}_{23} \\ 0 & 0 & 0 & 1 \end{vmatrix}, \tag{10}$$

где $q_{\sum} = q_1 + q_2$.

Для исходных данных, соответствующих вероятностям $P_0(0) = 1$; $P_1(0) = P_2(0) = P_3(0) = 0$, после первого шага вероятности состояний будут равны:

$$P_1(1) = 1 - q_{\sum} \;;\; P_1(1) = q_1 ;\; P_2(1) = q_2 ;\; P_3(1) = 0 . \tag{11}$$

Вероятности состояний после второго шага примут следующий вид:

$$P_0(2) = (1-q_{\sum})^2 + q_1 R_1 + q_2 R_2 ; P_1(2) = (1-q_{\sum})q_1 + q_2 r_{21} ; \tag{12}$$
$$P_2(2) = (1-q_{\sum})q_2 + q_1 r_{12} ;\; P_1(2) = q_1 \overline{R}_{13} + q_2 \overline{R}_{23} .$$

В соответствии с выражением (12) определим вероятность благополучного исхода от воздействия на систему внутренних угроз после второго шага преобразований, а именно:

$$P_{БИ}(2) = P_0(2) + P_1(2) + P_2(2).$$

Тогда вероятность неблагополучного исхода определится следующим образом:

$$Q_{БИ}(2) = 1 - P_{БИ}(2)$$

или с учетом (12):

$$Q_{БИ}(2) = q_1\overline{R}_{13} + q_2\overline{R}_{23}.$$

Используем полученные зависимости для определения вероятности благополучного исхода с учетом воздействия на АИС двух зависимых внутренних угроз.

Пример расчета. Определим вероятность благополучного исхода от воздействия на АИС двух зависимых внутренних угроз в соответствии с рис. 4.

Исходные данные для расчета: матрица вероятностей перехода (13); $P_0(0) = 1; P_1(0) = P_2(0) = P_3(0) = 0$;вероятность возникновения первой внутренней угрозы варьируется в пределах от $q_1 = 0{,}0$ до $q_1 = 0{,}8$;вероятность возникновения второй внутренней угрозы $q_2 = 0{,}2$; вероятность парирования второй внутренней угрозы $R_2 = 0{,}2$, а вероятности взаимного порождения внутренних угроз $r_{12} = r_{21} = 0{,}2$; вероятность парирования проявившейся внутренней угрозы $R_1 = 0{,}2$; количество шагов моделирования 12.

Результаты моделирования представлены на рис. 5.

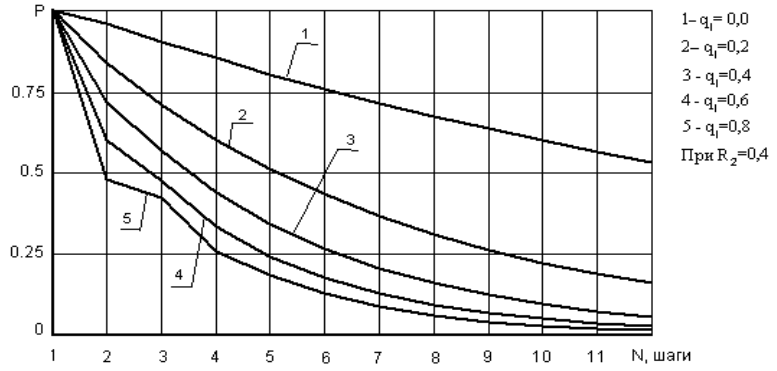

Рис. 5. Зависимость вероятности благополучного исхода от воздействия на АИС двух зависимых внутренних угроз при $R_1 = 0{,}2$

Пусть $R_1 = 0{,}6$. Тогда при исходных данных, соответствующих первой задаче, результаты моделирования будут иметь вид, представленный на рис. 6.

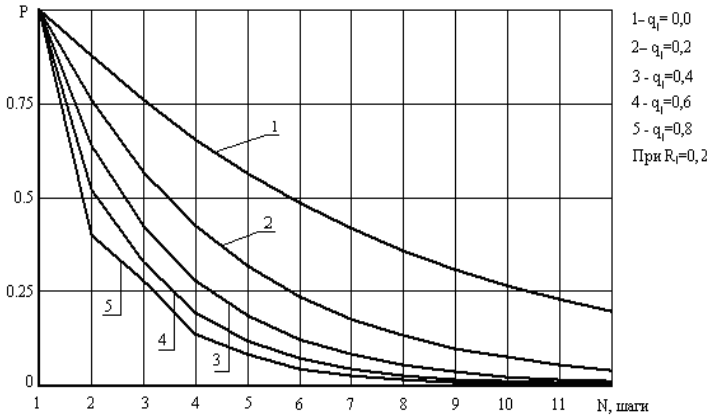

Рис. 6. Зависимость вероятности благополучного исхода от воздействия на АИС двух зависимых внутренних угроз при $R_1 = 0{,}6$

Анализ результатов моделирования, представленных на рис. 5 и 6 позволяет сделать следующие выводы:

- как и в случае, показанном на рис. 3, система может оказаться в поглощающем состоянии после второго и последующих шагов;
- с увеличением вероятности R_1 наблюдается устойчивое сближение графиков, для значений от $q_1 = 0{,}2$ до $q_1 = 0{,}8$ с графиком, для $q_1 = 0{,}0$;
- результаты моделирования показывают, что график при $q_1 = 0{,}0$, практически не изменяет своего положения с ростом R_1 (слабо выраженная тенденция роста);
- можно показать, что при $R_1 \to 1{,}0$ графики 2, 3, 4 и 5 (значения параметра $q_1 = 0{,}2 \div 0{,}8$), сливаются с графиком 1 (значение параметра $q_1 = 0{,}0$).

Определим указанную вероятность для исходных данных, рассмотренных в первой и второй задаче за исключением того, что будем изменять вероятность парирования второй проявившейся угрозы от $R_2 = 0{,}4$ до $R_2 = 0{,}6$, а вероятность R_1 – зафиксируем со значением $R_1 = 0{,}2$.

Результаты моделирования представлены на рис. 7 (где $R_2 = 0{,}4$) и рис. 8 (где $R_2 = 0{,}6$).

Анализ результатов моделирования, представленных на рис. 7 и 8 позволяет сделать следующие выводы:

- с увеличением вероятности R_2 наблюдается незначительный рост вероятности благополучного исхода от воздействия на АИС внутренних угроз во всем диапазоне изменения параметра q_1, т.е. для $q_1 = 0{,}0 \div 0{,}8$;
- анализ также показывает на отсутствие сближения графиков при изменении параметров q_1 и R_2, что свидетельствует о положительном влиянии параметра R_2 на вероятность благополучного исхода во всем диапазоне изменения параметра q_1.

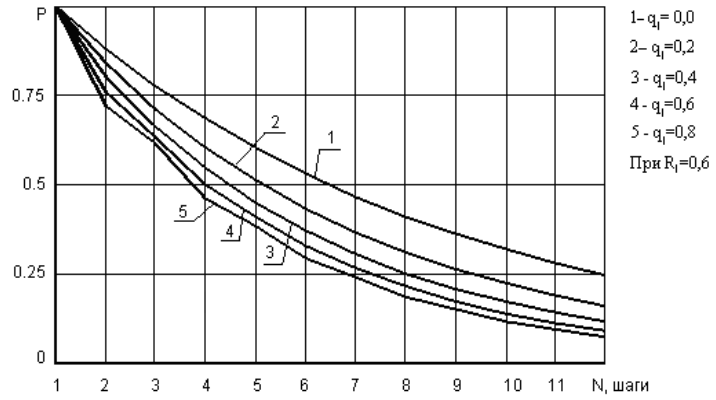

Рис. 7. Зависимость вероятности благополучного исхода от воздействия на АИС двух зависимых внутренних угроз при $R_2 = 0{,}4$

Таким образом, результаты моделирования показывают, что при аналогичных исходных данных с увеличением вероятности парирования проявившейся первой угрозы, т.е. R_1, все графики, приближаются к графику, полученному для $q_1 = 0{,}0$. При увеличении вероятности парирования второй проявившейся угрозы, т.е. R_2, все графики плавно смещаются в направлении увеличения вероятности благополучного исхода от воздействия внутренних угроз на АИС. Это свидетельствует о том, что у собственника конфиденциальной информации имеются различные варианты применения защитных механизмов. В зависимости от имеющихся материальных ресурсов, он может реализовать те из них, которые дают положительный наилучший эффект.

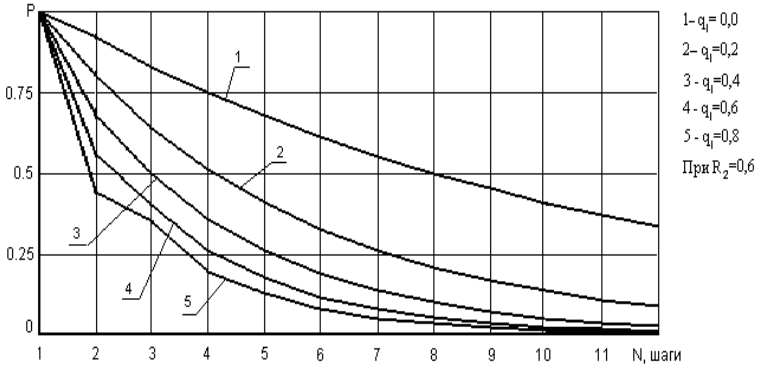

Рис. 8. Зависимость вероятности благополучного исхода от воздействия на АИС двух зависимых внутренних угроз при $R_2 = 0{,}6$

6. Общие выводы

Разработанные математические модели на основе марковских случайных процессов с дискретными состояниями позволяют получить количественные зави-

симости, характеризующие степень влияния внутренних угроз на безопасность информации ограниченного распространения.

Результаты моделирования показывают, что уже после второго шага система может оказаться в поглощающем состоянии, соответствующего реализации злоумышленником внутренней угрозы

Увеличение числа шагов процесса перехода системы из состояния в состояние не только увеличивает его длительность, но и число особых ситуаций, возникающих в результате воздействия на систему внутренних угроз, а, следовательно, и к росту вероятности оказаться в поглощающем, неблагополучном состоянии.

Собственник информации ограниченного распространения может использовать полученные количественные зависимости для разработки научно-обоснованных мероприятий по применению защитных механизмов в зависимости от имеющихся методов и средств, а также располагаемых материальных ресурсов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Тихонов, В.И., Миронов, М.А.* Марковские процессы. – М.: Советское радио,1997. – 488 с.

2. *Вентцель, С. Е*. Исследование операций. – М.: Советское радио,1972. – 550 с.

3. *Росенко, А.П.* Марковские модели оценки безопасности конфиденциальной информации с учетом воздействия на автоматизированную информационную систему внутренних угроз[Текст] / Росенко А.П. // Вестник Ставропольского государственного университета. – Ставрополь: СГУ, 2005. – С. 34-40.

4. *Росенко, А.П.* Научно-теоретические основы исследования влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированных информационных системах [Текс] / Росенко А.П. // Известия ТРТУ. Материалы VII международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2005. – С. 19-30.

5. Внутренние ИТ-угрозы в России 2006. www.infowatch.ru.

6. *Росенко, А.П., Клименко, Е.С.* О выборе критерия оценки эффективности функционирования системы защиты информации [Текст]/ Росенко А.П., Клименко Е.С. // Первая международная научно-техническая конференция. Инфотелекоммуникационные технологии в науке, производстве и образовании. – Ставрополь: Изд-во Сев-Кав. ГТУ, 2004. – С. 207-208.

УДК 683.34

Ю.К. Язов, Т.В. Григорьева

ПАРАДИГМА ПРЕДЕЛЬНОГО УЩЕРБА И ЕЕ ИСПОЛЬЗОВАНИЕ ПРИ ОЦЕНКЕ РИСКОВ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ

В данной статье рассматривается один из важных и актуальных вопросов развития методологии количественной оценки эффективности защиты информации – построение шкал комплексной оценки рисков нарушений безопасности информации на основе парадигмы предельного ущерба. Указанная парадигма широко используется в жизни при различных видах оценок. Ее суть заключается в установлении верхней границы шкалы оценок, выше которой значение оцениваемого параметра не влияет на выводы относительно объекта оценки (оцениваемого процесса, явления, события, уровня знаний и т.п.) и, в частности, относительно риска нарушения безопасности информации в компьютерной системе, определяемого,