УДК 681.518.3

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТЕЙ СОСТОЯНИЙ ФУНКЦИОНИРОВАНИЯ СРЕДСТВА КОНТЕНТНОГО АНАЛИЗА КАК ЭЛЕМЕНТА СИСТЕМЫ МОНИТОРИНГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.В. Попов, В.Н. Шамкин

Кафедра «Конструирование радиоэлектронных и микропроцессорных систем», ФГБОУ ВПО «ТГТУ»; posevik@yandex.ru

Представлена членом редколлегии профессором В.И. Коноваловым

Ключевые слова и фразы: интенсивности отказов и восстановления; информационная безопасность; инцидент и событие информационной безопасности; марковский случайный процесс; матрица переходов; переходные вероятности; состояния функционирования; средство контентного анализа.

Аннотация: Предложено использовать метод переходных вероятностей для вычисления возможности пребывания средств защиты информации, работающих в дискретном времени в системе мониторинга инцидентов информационной безопасности банка, в состояниях функционирования, обусловленных нарушениями их работы. Для средства контентного анализа выявлено множество возможных состояний функционирования и найдены их стационарные и нестационарные вероятности, которые в последующем могут быть использованы администратором безопасности в процессе принятия решений, а также при проектировании новых систем мониторинга.

Абберевиатуры

АБС – автоматизированная банковская система;	СЗИ – средство защиты информации;
БД – база данных;	СИБ – событие информационной безопасности;
ИБ – информационная безопасность;	СКА – средство контентного анализа;
ИИБ – инцидент информационной безопасности;	СКПВВ – средство контроля портов ввода-вывода;
ИнС – индексирующий сервер;	СМИИБ – система мониторинга инцидентов информационной безопасности.
МП – модуль-посредник;	
МПр – модуль проверки;	

Введение

Система мониторинга инцидентов информационной безопасности представляет собой подсистему АБС, в которую поступают на анализ сведения обо всех СИБ, происходящих в АБС, с целью выявления среди них ИИБ [1].

Как отмечалось в [2] на нижнем уровне СМИИБ располагаются различные программно-аппаратные СЗИ, собирающие данные о событиях ИБ в АБС: сканер безопасности; средство контентного анализа; средство контроля портов ввода-вывода; межсетевой экран; система обнаружения атак и др.

Изучению состояний функционирования СЗИ, а также их влияния на эффективность мониторинга инцидентов информационной безопасности банка посвящены работы [1–5].

Следует отметить, что подход к изучению технических систем с учетом изменения их состояний функционирования разработан профессором Ю.Л. Муромцевым, среди многочисленных публикаций которого отметим, например [6, 7].

С точки зрения надежности можно выделить два вида средств защиты – с дискретным и непрерывным временем их работы [3]. Рассуждения в статье проведем на примере СКА, принадлежащего к дискретному виду средств защиты.

Состояния функционирования средства контентного анализа

Средство контентного анализа, как программный комплекс, содержит в себе три основных активных программных компонента: модуль-посредник; индексирующий сервер и модуль проверки индекса, выполняющих некоторый набор функций [3]. Другие компоненты СКА, такие как хранилище данных и индекс, представляющие определенные структуры данных, необходимы для функционирования активных компонентов.

Рассмотрим одну из разновидностей СКА – систему аудита файлов, копируемых на съемные носители. В этой системе источником информации, подлежащей последующему контентному анализу, является другое СЗИ, а именно, СКПВВ. Такая система аудита используется для сбора информации о выносимых за пределы АБС банка файлах и для ее последующего анализа с целью выявления файлов, не соответствующих требованиям безопасности.

Характерной особенностью функционирования СКА является то, что его активные компоненты работают независимо и выполняют свои основные функции периодически, с разной частотой:

– модуль-посредник – функцию копирования файлов из БД СКПВВ в хранилище один раз в минуту;

– индексирующий сервер – функцию обновления индекса по расписанию (например три раза в сутки – в 7:00, 15:00 и 23:00) и по запросу администратора (по мере необходимости);

– модуль проверки – функцию проверки в режиме, аналогичном работе индексирующего сервера, но с небольшим запаздыванием.

Рассматривая СКА как объект исследования на надежность, отдельно проанализируем работу такого активного программного компонента, как МПр индекса. Его основная функция состоит в том, что модуль периодически обращается к индексу СКА с запросом, содержащим список контрольных слов, выражений и текстовых фрагментов, который составлен администратором. При обнаружении фактов несоблюдения политики безопасности МПр передает администратору соответствующее уведомление. В случае нештатного выполнения МПр этой функции (как показывает практика, весьма редких), администратор может передавать запрос в индекс вручную и получать соответствующие результаты, то есть может на некоторое время взять исполнение его функций МПр на себя. В этой связи представляется целесообразным принять допущение о том, что МПр надежен и постоянно находится в состоянии нормального функционирования.

В соответствии со сказанным, далее будем говорить о выполнении или невыполнении своих основных функций такими активными компонентами СКА, как МП и ИнС.

В процессе работы СКА происходят ошибки четырех видов [3].

1. Произошла несанкционированная очистка (обнуление) индекса СКА текущей БД СКПВВ.
2. Отсутствует реакция ИнС СКА на управляющие воздействия.

3. Невозможно осуществить копирование файлов из БД СКПВВ в хранилище данных СКА по причине отсутствия свободного места на жестком диске сервера, на котором развернуто (установлено) СКА.

4. Невозможно осуществить копирование файлов из БД СКПВВ в хранилище данных СКА по причине неудачной аутентификации МП в БД СКПВВ.

Первые две ошибки относятся к ИнС, а последние две – к МП.

Появляющаяся ошибка или ее устранение приводят к тому, что СКА из некоторого состояния функционирования, характеризуемого работой его компонентов, переходит в какое-то другое состояние. Каждое из них характеризуется некоторой эффективностью функционирования, когда в той или иной мере выполняется основная функция СКА. Существуют также состояния, называемые состояниями отказа, в которых основная функция не выполняется,

В любой момент времени СКА может находиться в одном из состояний, принадлежащем множеству возможных состояний функционирования *H*. Сформируем множество *H*, выявив эти состояния и пояснив смысл каждого из них.

Состояние нормального функционирования h_0 характеризует штатную работу МП и ИнС.

Состояние h_1 характерно для нормальной работы МП и некорректно завершенной работы ИнС, в результате чего появилась ошибка первого вида, фиксируемая в журнале работы ИнС. Из состояния h_0 в состояние h_1 переход происходит в случае несанкционированной перезагрузки аппаратного сервера, на котором установлено СКА как СЗИ, в момент обновления в СКА индекса (происходящего через строго определенные промежутки времени). В состоянии h_1 происходит несанкционированная очистка (обнуление) индекса текущей БД СКПВВ. При этом в h_1 полной утраты функциональности СКА не происходит, а снижается эффективность его работы. По окончании несанкционированной перезагрузки сервера, ИнС автоматически начинает повторное индексирование, до завершения которого ни МПр, ни администратор не могут получать информацию о событиях ИБ. После завершения индексирования в течение некоторого времени МПр производит повторный анализ проверенной ранее информации, поступившей в хранилище СКА к моменту перехода в состояние h_1, с выдачей администратору соответствующих сообщений. Лишь затем на проверку попадут недавно поступившие сведения о скопированных пользователями файлах на сменные носители. В этой связи выявление СКА фактов нарушения политики безопасности и реагирование на них администратора будут запаздывать.

Восстановление нормального функционирования СКА, то есть переход из состояния h_1 в состояние h_0, происходит по завершению повторного индексирования данных.

Состояние h_2 СКА характерно для нормальной работы МП и переставшего реагировать на управляющие воздействия ИнС. В результате чего появляется ошибка второго вида, фиксируемая в журнале работы ИнС. В состояние h_2 можно перейти из h_0 по различным причинам, например при чрезмерном увеличении размера индекса СКА. В этом случае ИнС не может завершить индексирование данных, начатое по расписанию или запросу администратора, тем самым препятствуя дальнейшему анализу модулем проверки копируемых файлов. Это означает, что СКА не выполняет такую функцию, как обнаружение СИБ.

Для восстановления реакции ИнС на управляющие воздействия администратору безопасности необходимо произвести перезагрузку аппаратного сервера, на

котором установлено СКА. В результате происходит переход СКА из состояния h_2 в работоспособное состояние h_0.

Состояние h_3 характерно для СКА, когда ИнС работает нормально, а МП не может осуществить копирование файлов из БД СКПВВ в хранилище данных СКА по причине отсутствия свободного места на жестком диске сервера, на котором расположено СКА. Переполнение жесткого диска может произойти при наличии на сервере нескольких программных комплексов различного назначения, работающих с большими объемами данных, при пониженном контроле со стороны персонала. При этом в журнале работы МП фиксируется ошибка третьего вида.

Если МП находится в состоянии h_3, вновь поступающие в СКА файлы, предназначенные для контентного анализа, не могут своевременно попасть в хранилище, и соответственно недоступны для последующего индексирования. Однако возможен поиск событий ИБ среди файлов, которые были скопированы в хранилище данных СКА и проиндексированы ранее. Таким образом, в состоянии h_3 выявление фактов нарушения политики безопасности будет запаздывать, что можно расценивать как снижение эффективности работы СКА.

Переход СКА в состояние h_0 из состояния h_3 происходит после освобождения администратором места на жестком диске сервера, на котором расположено СКА.

Состояние h_4 характеризует работу СКА, когда ИнС работает нормально, а МП не может осуществить копирование файлов из БД СКПВВ в хранилище СКА по причине неудачной аутентификации МП в БД СКПВВ. В журнал работы МП при этом заносится запись об ошибке четвертого вида.

Переход в h_4 из h_0 происходит из-за несанкционированного изменения прав доступа учетной записи, используемой СКА для подключения к БД СКПВВ, или из-за неверно введенных администратором в ходе переустановки, или обновления ПО СКА данных этой учетной записи (имени пользователя и пароля).

При этом не происходит полной утраты функциональности СКА и в полной мере справедливо сказанное в отношении снижения эффективности работы СКА для состояния h_3.

Из приведенных выше рассуждений видно, что каждый из компонентов СКА – МП и ИнС имеет по три состояния функционирования – по одному нормальному и по два с пониженной эффективностью.

Опишем далее состояния функционирования СКА, в которые возможен переход из состояний $h_1 - h_4$, характеризуемых нарушением функций одного из компонентов, в состояния, связанные с нарушением также функций и другого компонента. Эти состояния являются отказовыми, то есть такими, когда СКА полностью перестает выполнять свою основную функцию, связанную с обнаружением СИБ среди поступивших из СКПВВ файлов.

Состояние h_{13} характеризует некорректное завершение работы ИнС и невозможность МП осуществить копирование файлов из БД СКПВВ в хранилище СКА по причине отсутствия свободного места на жестком диске сервера, на котором расположено СКА. В журналах работы ИнС и МП фиксируются ошибки первого и третьего видов соответственно, при этом первая ошибка появляется раньше третьей.

Для состояния h_{14} СКА характерно некорректное завершение работы ИнС и невозможность МП осуществить копирование файлов из БД СКПВВ в хранилище СКА по причине неудачной аутентификации МП в БД СКПВВ, что в совокупно-

сти не позволяет выполнять основную функцию СКА. В журналы работы ИнС и МП заносятся записи о последовательно произошедших ошибках первого и четвертого видов соответственно.

Состояние h_{23} характерно для ИнС, переставшего реагировать на управляющие воздействия, и МП, неспособного копировать файлы из БД СКПВВ в хранилище СКА по причине отсутствия свободного места на жестком диске сервера, на котором развернуто СКА. В журналы работы ИнС и МП заносятся записи о последовательно произошедших ошибках второго и третьего видов.

Состояние h_{24} характерно для ИнС, переставшего реагировать на управляющие воздействия, и МП, неспособного копировать файлы из БД СКПВВ в хранилище СКА по причине неудачной аутентификации в БД. При этом в журналы работы ИнС и МП заносятся записи о последовательно произошедших ошибках второго и четвертого видов.

Возможны также и другие состояния СКА, а именно h_{31}, h_{32}, h_{41}, h_{42}, в которых последовательность произошедших нарушений основных функций активных компонентов СКА иная.

Таким образом, множество возможных состояний функционирования СКА имеет вид

$$H = \{h_0, h_1, h_2, h_3, h_4, h_{13}, h_{14}, h_{23}, h_{24}, h_{31}, h_{32}, h_{41}, h_{42}\}. \quad (1)$$

Смена состояний СКА происходит в случайные моменты времени по различным причинам независимо друг от друга. Как нарушения в работе, так и устранение возникающих ошибок возможны как без участия, так и с участием человека.

Используя множество (1), можно описать поведение СКА, как объекта с дискретным временем работы, в виде ориентированного графа, представленного на рис. 1. Вершины графа характеризуют возможные состояния СКА, а в качестве весов дуг графа указываются соответствующие вероятности переходов из одних состояний в другие за некоторый промежуток времени Δt, определяющий дискретный (потактовый) режим его работы. При этом прямоугольниками выделены состояния, соответствующие двум ошибкам каждого из компонентов СКА – модуля-посредника и индексирующего сервера.

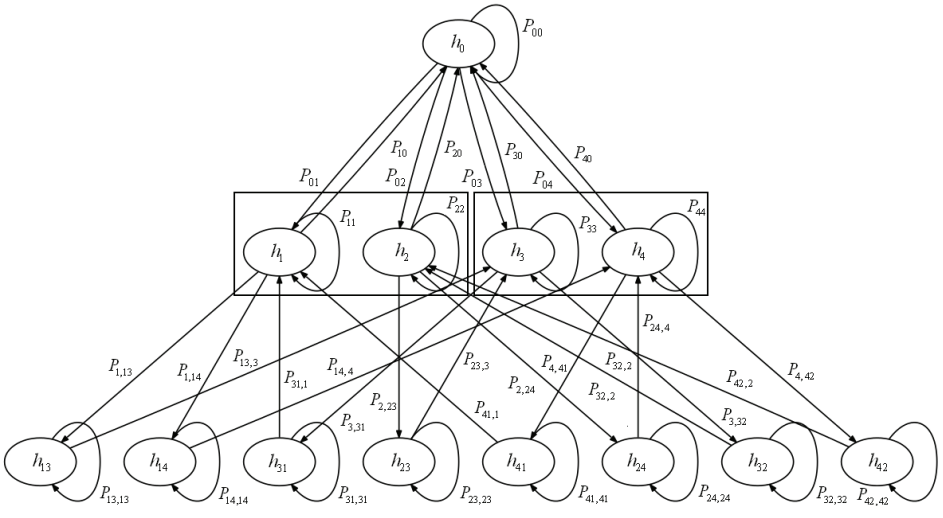

Рис. 1. Диаграмма переходных вероятностей СКА

Здесь $P_{i,i}$, $i = 0,1,2,3,4,13,14,23,24,31,32,41,42$ – вероятности сохранения состояний $h_0, h_1, h_2, h_3, h_4, h_{13}, h_{14}, h_{23}, h_{24}, h_{31}, h_{32}, h_{41}, h_{42}$ за время Δt; $P_{i,j}$, $i, j = 0,1,2,3,4,13,14,23,24,31,32,41,42$, $i \neq j$ – вероятности переходов из состояния h_i в состояние h_j за время Δt.

Конкретный вид диаграммы вероятностей переходов, представленной на рис. 1, обусловлен ограниченным режимом обслуживания СКА в процессе возникающих нарушений, то есть тем, что устройство обслуживает один ремонтник.

Вероятности $P_{i,j}$, $i \neq j$, описывают переходы, связанные с возникновением нарушений определенного вида или их устранением за время Δt. Предполагается, что время нормальной работы отдельных компонентов СКА и время устранения возникающих в них нарушений являются случайными величинами, имеющими показательные законы распределения. Интенсивности возникновения λ_k k-го нарушения и его устранения μ_k, $k = \overline{1,4}$, считаются заданными. Соответственно при определении конкретных вероятностей перехода $P_{i,j}$ используются формулы, характеризующие конкретные нарушения или их устранения, то есть вероятности того, что за время Δt произойдет k-я ошибка или она будет устранена:

$$Q_k(\Delta t) = 1 - \mathrm{e}^{-\lambda_k \Delta t}, \quad P_k(\Delta t) = 1 - \mathrm{e}^{-\mu_k \Delta t}, \quad k = \overline{1,4}. \tag{2}$$

Вероятности $P_{i,i}$ определяются с использованием деревьев состояний, характеризующих переходы СКА из различных состояний функционирования в другие за время Δt, с учетом полной группы событий, определяющих условия нахождения СКА в одном из возможных состояний функционирования.

Определение нестационарных вероятностей состояний функционирования СКА

Поскольку СКА является системой с дискретным временем, то для анализа ее надежности с точки зрения возможности нахождения СКА в различных состояниях функционирования $h \in H$ применим метод переходных вероятностей [8], который требует знания вероятностей переходов СКА из одного состояния в другое за некоторое время Δt, определяющее дискретный (потактовый) режим его работы. В нашем случае Δt = 8 ч характеризует длину одного такта m.

Целью последующего анализа является определение вектор-функции вероятностей $p(m)$, характеризующей потактовое изменение состояний $h \in H$,

$$p(m) = (p_0(m), p_1(m), p_2(m), p_5(m), p_4(m), p_{13}(m), p_{14}(m), p_{23}(m), p_{24}(m), p_{31}(m), p_{32}(m), p_{41}(m), p_{42}(m)), \quad m = 0, 1, 2, \ldots, \tag{3}$$

и вектора стационарных вероятностей $\overline{p}$, характеризующего их установившиеся значения при $m \to \infty$,

$$\overline{p} = (\overline{p}_0, \overline{p}_1, \overline{p}_2, \overline{p}_3, \overline{p}_4, \overline{p}_{13}, \overline{p}_{14}, \overline{p}_{23}, \overline{p}_{24}, \overline{p}_{31}, \overline{p}_{32}, \overline{p}_{41}, \overline{p}_{42}). \tag{4}$$

Использование этого метода предполагает знание матрицы переходов, соответствующей диаграмме переходных вероятностей СКА (см. рис. 1):

$$M = \begin{Vmatrix} P_{00} & P_{01} & P_{02} & P_{03} & P_{04} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{10} & P_{11} & 0 & 0 & 0 & P_{1,13} & P_{1,14} & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{20} & 0 & P_{22} & 0 & 0 & 0 & 0 & P_{2,23} & P_{2,24} & 0 & 0 & 0 & 0 \\ P_{30} & 0 & 0 & P_{33} & 0 & 0 & 0 & 0 & 0 & P_{3,31} & P_{3,32} & 0 & 0 \\ P_{40} & 0 & 0 & 0 & P_{44} & 0 & 0 & 0 & 0 & 0 & 0 & P_{4,41} & P_{4,42} \\ 0 & 0 & 0 & P_{13,3} & 0 & P_{13,13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & P_{14,4} & 0 & P_{14,14} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & P_{23,3} & 0 & 0 & 0 & P_{23,23} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & P_{24,4} & 0 & 0 & 0 & P_{24,24} & 0 & 0 & 0 & 0 \\ 0 & P_{31,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{31,31} & 0 & 0 & 0 \\ 0 & 0 & P_{32,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{32,32} & 0 & 0 \\ 0 & P_{41,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{41,41} & 0 \\ 0 & 0 & P_{42,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{42,42} \end{Vmatrix}. \quad (5)$$

Матрица (5) является квадратной (13 × 13), число ее строк и столбцов определяется числом возможных состояний функционирования СКА, образующих множество H (1). Столбец определяет вероятность сохранения i-го состояния и перехода в него из других состояний при срабатывании в один такт от $(m-1)$ к m. Строка определяет распределение вероятностей каждого из состояний СКА, то есть вероятность сохранения i-го состояния и вероятности перехода из i-го состояния в другие. Сумма членов каждой строки равна 1, то есть матрица M является стохастической.

Поскольку матрица M является стохастической, то это позволяет рассматривать ее как матрицу переходных вероятностей цепи Маркова с дискретным временем и конечным множеством состояний [8].

Начальное распределение вероятностей $M(0)$ состояний функционирования $h \in H$, характеризующее возможность нахождения СКА в первоначальный момент времени ($m = 0$) в каком-либо состоянии, определяется в общем виде матрицей-строкой

$$M(0) = \left\| p_0(0), p_1(0), p_2(0), p_5(0), p_4(0), p_{13}(0), p_{14}(0), p_{23}(0), p_{24}(0), \right.$$
$$\left. p_{31}(0), p_{32}(0), p_{41}(0), p_{42}(0) \right\|. \quad (6)$$

Причем $\sum_i P_i(0) = 1$, где $P_i(0)$ – вероятность нахождения СКА в начальный момент времени $(m = 0)$ в состоянии h_i, $i = 0,1,2,3,4,13,14,23,24,31,32,41,42$.

Например, если в начальный момент времени все компоненты СКА исправны, а, следовательно, и СКА находится в состоянии нормального функционирования h_0, то

$$M(0) = \left\| 1,0,0,0,0,0,0,0,0,0,0,0,0 \right\|. \quad (7)$$

Вероятность $P(m)_i$ нахождения СКА в состоянии h_i после m последовательных тактов в общем виде определяется формулой

$$P(m)_i = M(0)M^m D_i, \quad i = 0,1,2,3,4,13,14,23,24,31,32,41,42, \quad (8)$$

где D_i – вектор-столбец, элементами которого являются «0» или «1», причем «1» соответствует анализируемому состоянию h_i.

Например, состоянию h_1 соответствует вектор-столбец

$$D_1 = \left\| 0,1,0,0,0,0,0,0,0,0,0,0,0 \right\|^{\mathrm{T}},$$

где т – символ транспонирования.

Конкретный вид матрица (5) приобрела после вычисления соответствующих значений вероятностей перехода $P_{i,j}$, $i, j = 0,1,2,3,4,13,14,23,24,31,32,41,42$. Значения этих вероятностей вычислены по формулам (2) с использованием следующих данных для λ_i и μ_i, $i = \overline{1,4}$: $\lambda_1 = 4{,}95 \cdot 10^{-4}$ и $\mu_1 = 0{,}58$; $\lambda_2 = 7{,}48 \cdot 10^{-4}$ и $\mu_2 = 0{,}2$; $\lambda_3 = 5{,}16 \cdot 10^{-4}$ и $\mu_3 = 0{,}09$; $\lambda_4 = 6{,}43 \cdot 10^{-4}$ и $\mu_4 = 0{,}17$.

Таким образом,

$$M = 10^{-3} \times \begin{Vmatrix} 980{,}83 & 3{,}95 & 5{,}96 & 4{,}12 & 5{,}13 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 990{,}34 & 0{,}403 & 0 & 0 & 0 & 4{,}12 & 5{,}13 & 0 & 0 & 0 & 0 & 0 & 0 \\ 794{,}84 & 0 & 195{,}9 & 0 & 0 & 0 & 0 & 4{,}12 & 5{,}13 & 0 & 0 & 0 & 0 \\ 524{,}79 & 0 & 0 & 465{,}3 & 0 & 0 & 0 & 0 & 0 & 3{,}95 & 5{,}96 & 0 & 0 \\ 739{,}2 & 0 & 0 & 0 & 250{,}88 & 0 & 0 & 0 & 0 & 0 & 0 & 3{,}95 & 5{,}96 \\ 0 & 0 & 0 & 990{,}34 & 0 & 9{,}66 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 990{,}34 & 0 & 9{,}66 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 794{,}85 & 0 & 0 & 0 & 205{,}15 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 794{,}85 & 0 & 0 & 0 & 205{,}15 & 0 & 0 & 0 & 0 \\ 0 & 524{,}79 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 475{,}21 & 0 & 0 & 0 \\ 0 & 0 & 524{,}79 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 475{,}21 & 0 & 0 \\ 0 & 739{,}2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 260{,}8 & 0 \\ 0 & 0 & 739{,}2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 260{,}8 \end{Vmatrix}. \quad (9)$$

Задав вектор начального состояния $M(0)$ вида (7) и задавая вектора D_i для состояний $h_i \in H$, $i = 0,1,2,3,4,13,14,23,24,31,32,41,42$, и используя матрицу (9) можно определить по формуле (8) вероятности нахождения СКА в каждом из этих состояний через любое количество тактов m = 1, 2, …, а в итоге определить вектор-функцию $p(m)$ вероятностей состояний вида (3).

Например, для вектора $M(0)$ вида (7), определяющего начальное состояние h_0, и состояния h_2, характеризуемого матрицей-столбцом $D_2 = \|0,0,1,0,0,0,0,0,0,0,0,0,0\|^{\mathrm{T}}$, после двух тактов вероятность нахождения СКА в состоянии h_2 равна

$$P(2)_2 = M(0)M^2 D_2 = 7{,}02 \cdot 10^{-3}.$$

Таким образом, после двух тактов m = 2 (через 16 ч работы), с вероятностью $7{,}02 \cdot 10^{-3}$ СКА окажется в состоянии функционирования h_2, характеризуемом нормальной работой МП и не реагирующим на управляющие воздействия ИнС. В результате появится ошибка второго вида, которая зафиксируется в журнале работы ИнС, и будет выдано соответствующее сообщение об ошибке [3].

Проведя подобные вычисления при m = 2 для других состояний функционирования можно получить вектор, характеризующий распределение вероятностей по всем состояниям через два такта,

$$p(2) = (0{,}98,\ 3{,}88 \cdot 10^{-3},\ 7{,}02 \cdot 10^{-3},\ 5{,}96 \cdot 10^{-3},\ 6{,}32 \cdot 10^{-3},\ 1{,}63 \cdot 10^{-5},\ 2{,}03 \cdot 10^{-5},$$
$$2{,}46 \cdot 10^{-5},\ 3{,}06 \cdot 10^{-5},\ 1{,}63 \cdot 10^{-5},\ 2{,}46 \cdot 10^{-5},\ 2{,}03 \cdot 10^{-5},\ 3{,}06 \cdot 10^{-5}).$$

Выполнив вычисления для различных m, в итоге получим функцию вида (3).

При увеличении m вероятности $p_i(m)$, $i = 0,1,2,3,4,13,14,23,23,31,32,41,42$, изменяются. Например, аппроксимированный график зависимости вероятности $p_0(m)$ состояния нормального функционирования СКА h_0 от числа тактов m представлен на рис. 2.

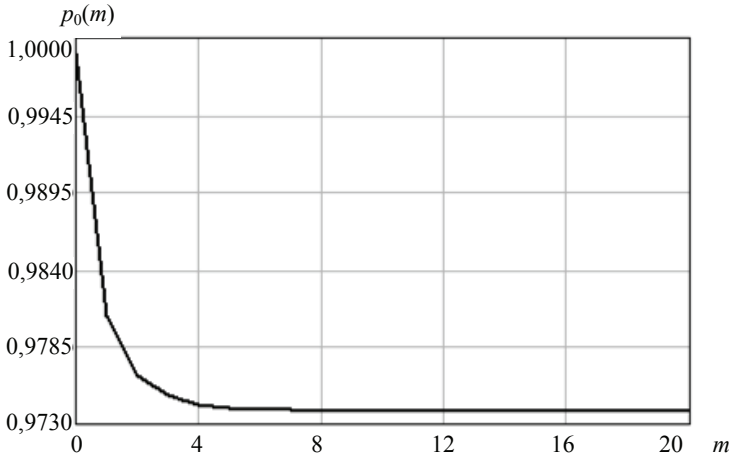

Рис. 2. Изменение вероятности состояния h_0 во времени (за m = 20 тактов)

Определение предельных (стационарных) вероятностей состояний функционирования

Для эргодических марковских процессов с дискретным временем и конечным множеством состояний функционирования, к числу которых принадлежит рассматриваемый нами процесс, при $m \to \infty$ предельное (стационарное) распределение вероятностей $\overline{p}_i$ между состояниями $h_i \in H$ не зависит от начального состояния объекта [9]. Это свойство позволяет определить распределение вероятностей $\overline{p}_i$ (4) путем решения системы алгебраических уравнений, составленной по матрице переходов M.

Для средств контентного анализа данная система уравнений в общем виде записывается следующим образом:

$$\begin{cases} \overline{p}_0 = P_{00}\overline{p}_0 + P_{10}\overline{p}_1 + P_{20}\overline{p}_2 + P_{30}\overline{p}_3 + P_{40}\overline{p}_4, \\ \overline{p}_1 = P_{01}\overline{p}_0 + P_{11}\overline{p}_1 + P_{31,1}\overline{p}_{31} + P_{41,1}\overline{p}_{41}, \\ \overline{p}_2 = P_{02}\overline{p}_0 + P_{22}\overline{p}_2 + P_{32,2}\overline{p}_{32} + P_{42,2}\overline{p}_{42}, \\ \overline{p}_3 = P_{03}\overline{p}_0 + P_{33}\overline{p}_3 + P_{13,3}\overline{p}_{13} + P_{23,3}\overline{p}_{23}, \\ \overline{p}_4 = P_{04}\overline{p}_0 + P_{44}\overline{p}_4 + P_{14,4}\overline{p}_{14} + P_{24,4}\overline{p}_{24}, \\ \overline{p}_{13} = P_{1,13}\overline{p}_1 + P_{13,13}\overline{p}_{13}, \\ \overline{p}_{14} = P_{1,14}\overline{p}_1 + P_{14,14}\overline{p}_{14}, \\ \overline{p}_{23} = P_{2,23}\overline{p}_2 + P_{23,23}\overline{p}_{23}, \\ \overline{p}_{24} = P_{2,24}\overline{p}_2 + P_{24,24}\overline{p}_{24}, \\ \overline{p}_{31} = P_{3,31}\overline{p}_3 + P_{31,31}\overline{p}_{31}, \\ \overline{p}_{32} = P_{3,32}\overline{p}_3 + P_{32,32}\overline{p}_{32}, \\ \overline{p}_{41} = P_{4,41}\overline{p}_4 + P_{41,41}\overline{p}_{41}, \\ \overline{p}_{42} = P_{4,42}\overline{p}_4 + P_{42,42}\overline{p}, \end{cases} \quad (10)$$

причем $\overline{p}_0 + \overline{p}_1 + \overline{p}_2 + \overline{p}_3 + \overline{p}_4 + \overline{p}_{13} + \overline{p}_{14} + \overline{p}_{23} + \overline{p}_{24} + \overline{p}_{31} + \overline{p}_{32} + \overline{p}_{41} + \overline{p}_{42} = 1$,
где $\overline{p}_i$, $i = 0,1,2,3,4,13,14,23,24,31,32,41,42$ – искомые предельные вероятности.

В результате решения системы (10), в которую подставлены конкретные значения $P_{i,j}$, $i,j = 0,1,2,3,4,13,14,23,24,31,32,41,42$, получены следующие значения предельных (стационарных) вероятностей состояний функционирования:

$$\overline{p}_0 = 0{,}974;\ \overline{p}_1 = 3{,}906 \cdot 10^{-3};\ \overline{p}_2 = 7{,}329 \cdot 10^{-3};\ \overline{p}_3 = 7{,}595 \cdot 10^{-3};\ \overline{p}_4 = 6{,}752 \cdot 10^{-3};$$

$$\overline{p}_{13} = 1{,}626 \cdot 10^{-5};\ \overline{p}_{14} = 2{,}025 \cdot 10^{-5};\ \overline{p}_{23} = 3{,}8 \cdot 10^{-5};\ \overline{p}_{24} = 4{,}733 \cdot 10^{-5};$$

$$\overline{p}_{31} = 5{,}718 \cdot 10^{-5};\ \overline{p}_{32} = 8{,}629 \cdot 10^{-5};\ \overline{p}_{41} = 3{,}608 \cdot 10^{-5};\ \overline{p}_{42} = 5{,}446 \cdot 10^{-5}.$$

Выводы

1. Располагая сведениями о нестационарных и стационарных вероятностях нахождения СКА в различных состояниях функционирования, обусловленных нарушениями его работы, администратор безопасности может более качественно прогнозировать во времени его поведение. Имеются в виду как периоды, соответствующие запуску СКА, так и периоды установившейся работы.

2. Такой прогноз позволяет администратору сосредоточить внимание на наиболее значимых угрозах нарушения работоспособности СКА, благодаря чему принимаются более взвешенные решения о выявлении инцидентов информационной безопасности и последующем реагировании на них.

Список литературы

1. Попов, С.В. О влиянии состояний функционирования средств защиты информации на эффективность мониторинга инцидентов информационной безопасности банка / С.В. Попов, В.Н. Шамкин // Вестн. Тамб. гос. техн. ун-та. – 2011. – Т. 17, № 2. – С. 297–303.

2. Попов, С.В. Мониторинг состояний функционирования средств защиты информации в информационной системе / С.В. Попов, В.Н. Шамкин // Тр. междунар. науч.-техн. конф. «Современные информационные технологии» “Contemporary Information Technologies” (Computer-Based Conference) / Пенз. гос. технолог. акад. – Пенза, 2011. – Вып. 13. – С. 165–168.

3. Попов, С.В. Методика мониторинга надежностных показателей средств защиты информации в банке по данным их текущей эксплуатации / С.В. Попов, В.Н. Шамкин // Вопр. соврем. науки и практики. Ун-т им. В.И. Вернадского. – 2012. – № 1(37). – С. 64–75.

4. Попов, С.В. Оценка работоспособности средств защиты информации / С.В. Попов, В.Н. Шамкин // Прогрессивные технологии и перспективы развития : сб. мат. 2-й междунар. науч.-практ. конф., г. Тамбов, 5 нояб. 2010 г. / Тамб. гос. техн. ун-т. – Тамбов, 2010. – С. 50–51.

5. Попов, С.В. Возможные состояния функционирования средств защиты информации в системе мониторинга инцидентов информационной безопасности / С.В. Попов, В.Н. Шамкин // Новые технологии и инновационные разработки: мат. 4-й межвуз. науч.-практ. конф., г. Тамбов, 13 мая 2011 г. / Тамб. гос. техн. ун-т. – Тамбов, 2011. – С. 69–72.

6. Муромцев, Ю.Л. Моделирование и оптимизация технических систем на множестве состояний функционирований : монография / Ю.Л. Муромцев, Л.Н. Ляпин, У.В. Попова. – Воронеж : Изд-во Воронеж. гос. ун-та, 1993. – 144 с.

7. Муромцев, Ю.Л. Идентификация моделей, учитывающих изменение состояний функционирования / Ю.Л. Муромцев, Л.П. Орлова, Д.Ю. Муромцев // Обработка сигналов и полей. – 2000. – № 3. – С. 45–48.

8. Левин, Б.Р. Теория надежности радиотехнических систем (математические основы) / Б.Р. Левин. – М. : Сов. радио, 1978. – 264 с.

9. Надежность автоматизированных систем управления : учеб. пособие для вузов / И.О. Атовмян [и др.] ; под ред. Я.А. Хетагурова. – М. : Высш. школа, 1979. – 287 с.

Identification of the Probabilities of Functioning State by Means of Content Analysis as an Element of Monitoring over Information Security Incidents

S.V. Popov, V.N. Shamkin

Department "Designing of Radio-Electronic and Microprocessor Systems", TSTU, posevik@yandex.ru

Key words and phrases: failure and recovery rates; information security; incident and event of information security; Markov random process; transition matrix; transition probabilities; the state of operation; content analysis means.

Abstract: It is offered to use a method of transitive probabilities to calculate the possibility of information security devices, working in discrete time in the system of monitoring over the bank information security incidents, to remain in the state of operation caused by malfunctions in their work. For the content analysis we have identified the set of possible functioning conditions and their stationary and non-stationary probabilities which can be used by the security administrator in decision-making process, and for designing new systems of monitoring.

Bestimmung der Wahrscheinlichkeiten der Zustände des Funktionierens des Mittels der Kontentanalyse als Element des Systems des Monitorings der Zwischenfälle der Informationssicherheit

Zusammenfassung: Es ist vorgeschlagen, die Methode der Übergangswahrscheinlichkiten für die Berechnung der Möglichkeit des Vorhandenseines der Mittel des Informationsschutzes, die in der Diskretenzeit im System des Monitorings der Zwischenfälle der Informationssicherheit der Bank arbeiten, in den Zuständen des Funktionierens, die von ihrer Arbeit verletzungsbedingt sind, zu benutzen. Für das Mittel der Kontentenanalyse sind viele mögliche Zustände des Funktionierens gezeigt und ihre stationäre und unstationäre Wahrscheinlichkeiten gefunden, die später vom Administrator der Sicherheit im Prozess der Beschlußfassung und auch bei der Projektierung der neuen Monitoringssysteme benutzt werden können.

Détermination des probabilités des états du fonctionnement du moyen de l'analyse de content comme élement du système de monitoring des incidents de la sécurité informatique

Résumé: Est proposé l'emploi de la méthode des probabilités de transition pour le calcul de la possibilité de la présence des moyens de la protection de l'information fonctionnant dans le régime discret du système de monitoring des incidents de la sécurité informatique de la banque dans les états du fonctionnement conditionnés des erreurs de leur fonctionnement. Pour le moyen de l'analyse de content est déduite une multitude des états possibles du fonctionnement et sont trouvées leurs probabilités stationnaires et non-stationnaires qui peuvent ensuite être utilisées par l'administrateur de la sécurité lors du processus de l'obtention des solutions ainsi que lors de la conception de nouveaux systèmes de monitoring.

Авторы: ***Попов Сергей Викторович*** – соискатель кафедры «Конструирование радиоэлектронных и микропроцессорных систем»; ***Шамкин Валерий Николаевич*** – доктор технических наук, профессор кафедры «Конструирование радиоэлектронных и микропроцессорных систем», ФГБОУ ВПО «ТГТУ».

Рецензент: ***Муромцев Дмитрий Юрьевич*** – доктор технических наук, профессор, заведующий кафедрой «Конструирование радиоэлектронных и микропроцесссорных систем», ФГБОУ ВПО «ТГТУ».