В.В. Меньших, **О.В. Толстых**
доктор физико-математических наук,
профессор

МОДЕЛЬ РАСПРОСТРАНЕНИЯ И УСТРАНЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

MODEL OF DISTRIBUTION AND ELIMINATION OF INFORMATION SECURITY THREATS ON INFORMATION OBJECT

Предложена модель распространения различных типов угроз информационной безопасности на объекте информатизации и их устранения средствами системы защиты информации.

The model of distribution of various types of threats of information security on an object of informatization is presented and the ways of their elimination by means of an information security system are offered.

Введение. В настоящее время современные информационные технологии активно внедряются в деятельность органов внутренних дел. Однако использование этих технологий, обеспечивая повышение эффективности решения служебных задач сотрудниками, вместе с тем существенно увеличивает риск возникновения угроз информационной безопасности (ИБ) на объектах информатизации. В целях противодействия этим угрозам создаются системы защиты информации (СЗИ) [1].

В связи с этим актуальной является задача выбора варианта системы защиты информации (СЗИ) на объекте информатизации. В интересах решения этой задачи необходимо разработать модель, позволяющую оценивать не только процесс распространения, но и процесс устранения угроз.

Объект информатизации в общем случае включает в себя локальные вычислительные сети, отдельные автоматизированные рабочие места, вспомогательные технические средства и системы. Каждый элемент объекта информатизации может оказаться объектом воздействия нарушителей или оказаться вовлеченным в процесс распространения угроз информационной безопасности в связи с тесной взаимосвязанностью элементов между собой и их территориальным расположением. При этом источники угроз при взаимодействии с элементами объекта информатизации могут порождать различные угрозы этим элементам. Например, некоторые вредоносные программы воздействуют только на файлы определенного типа. Поэтому компьютер, в памяти которого нет файлов данного типа, сам не подвергаясь угрозе, выступает в качестве распространителя угрозы.

Частично данная задача решалась в [2—5], где использовался аппарат теории графов, теории сетей Петри и теории автоматов [6, 7], но в этих публикациях не учитывалась описанная выше особенность распространения угроз ИБ на объектах информатизации, моделирование которой осуществляется в настоящей статье.

Процесс моделирования включает несколько этапов.

Начальный этап: разработка графовой модели объекта информатизации. В каждом объекте информатизации могут быть выделены отдельные компоненты:

совокупность информационных средств, различающихся информационными ресурсами и способами их обработки (K);

совокупность вспомогательных технических средств, обеспечивающих функционирование информационных систем (V);

персонал (L).

Каждый из компонентов в свою очередь может быть разделен на множество элементов, которые могут подвергаться различным угрозам ИБ. Следовательно, объект информатизации представляет собой многоуровневую иерархическую систему.

Между элементами рассматриваемой системы существуют различного вида взаимоотношения, которые могут способствовать распространению угроз ИБ.

Поэтому для решения задачи обеспечения ИБ объекта информатизации необходимо выявить взаимоотношения между отдельными элементами для изучения их влияния на показатели обеспечения ИБ объекта информатизации в целом в интересах последующей оптимизации этих показателей.

Взаимоотношения между отдельными элементами являются проявлением осуществляемых политик безопасности информационных систем, используемых на данном объекте информатизации. Обратимся к рассмотрению только тех взаимоотношений между элементами компонентов объекта информатизации, которые влияют на распространение угроз ИБ на этом объекте.

Традиционно все взаимоотношения между элементами систем любой природы сводятся к бинарным отношениям следующих основных видов [8]:

топологическим (T), характеризующим отношения соответствия элементов друг другу;

функциональным (F), характеризующим существование соответствия между элементами, в частности отношения вида «иметь функцию»;

информационным (I), характеризующим отношения передачи информации между элементами;

временным, характеризующим причинно-следственные отношения между элементами, в частности отношения типа «завершиться ранее начала выполнения другого действия».

Временные отношения описывают причинно-следственные связи между элементами объекта информатизации, т. е. всегда являются проявлением существующих информационных и функциональных отношений в конкретных ситуациях использования информационных систем, например решении прикладных задач. Следовательно, учет всех информационных и функциональных отношений автоматически приведет к учету и всех временных отношений. Поэтому временные отношения в дальнейшем в работе не рассматриваются.

Данные бинарные отношения можно задать в виде графа $G = (GV, GE, h)$ с цветными дугами. Вершины $GV = L \cup V \cup K$ соответствуют множеству всех элементов объекта информатизации, дуги $GE = T \cup F \cup I$ — множеству всех отношений; h — функция задания цвета дуг, соответствующая типам угроз информационной безопасности.

Полученный граф $G = (GV, GE, h)$ описывает общую структуру процесса распространения угроз на объекте информатизации. Для более гибкого описания этого процесса преобразуем полученный граф в Петри-подобную сеть.

1-й этап: разработка сетевой модели распространения угроз информационной безопасности.

Преобразуем граф $G = (GV, GE, h)$ в цветную сеть $\Psi_1 = (\Sigma, \Theta^{(1)}, h, \lambda_1, \eta_1)$ следующим образом:

- множество вершин $v_i \in GV$, соответствующее элементам объекта информатизации, преобразуем во множество позиций $\sigma_i \in \Sigma_1$;

- множество дуг $e_i \in GE$, отражающих возможность распространения угроз информационной безопасности, преобразуем во множество переходов где $\theta_i \in \Gamma_1^{(1)}$, при этом в отличие от классических сетей, где цветными являются только фишки, будем считать, что переходы так же являются цветными.

Функцию задания цвета переходов будем обозначать, как и в графе, *h*, которая задавала цвета дугам этого графа. Отношение инцидентности вершин и дуг в графе G преобразуем в обобщенные функции входов и выходов η_1 и λ_1 соответственно:

если вершина v_j, соответствующая позиции σ_j, является началом дуг $e_{ji}, e_{j2},\ldots,e_{jp}$, которые были преобразованы в переходы $\theta_{j1}, \theta_{j2},\ldots, \theta_{jp}$, то

$$\eta_1(\theta_{ji}) = \sigma_j,\ j_i = 1,...,\mathrm{p};\ \lambda_1(\sigma_j) = \{\theta_{j1}, ..., \theta_{jp}\};$$

если вершина v_k, соответствующая позиции σ_k, — конец дуг $\theta_{ki}, \theta_{k2},\ldots,\theta_{kp}$, то

$$\lambda_1(\theta_{ki}) = \sigma_k,\ k_i = 1,...,\mathrm{p};\ \eta_1(\sigma_k) = \{\theta_k, ..., \theta_{kp}\}.$$

Если на объекте информатизации существует угроза определенного типа, то будем считать, что эта позиция маркирована фишкой, цвет которой соответствует типу угрозы (переходы и фишки, соответствующие одному типу угроз, окрашиваются в один и тот же цвет). Будем считать, что на множестве позиций задана функция $\mu = (\mu^i, \mu, ..., \mu^n) : \sigma \to N$, где $\mu^i(\sigma)$ — количество фишек *i*-го цвета в позиции σ.

В соответствии с классической теорией сетей естественно предположить, что переход θ цвета h^i разрешен, если входная позиция этого перехода $\sigma' = \eta(t)$ имеет $\mu(\sigma') \rangle 0$, т.е. во входе позиции перехода θ есть хотя бы одна фишка того же цвета, что и переход θ.

Срабатывание перехода θ означает изменение маркировки его входной позиции σ' и его выходной позиции σ'' следующим образом:

$$\mu^i(\sigma') := \mu^i(\sigma') - 1,\ \mu^i(\sigma'') := \mu^i(\sigma'') + 1.$$

Анализ показывает, что сетевая модель в данном виде не может быть использована для моделирования распространения угроз, т.к. допускает возможность существования конфликтов.

Действительно, если из позиции, соответствующей элементу объекта информатизации, фишка, моделирующая угрозу ИБ *i*-го типа, может распространяться на несколько других элементов, это приводит к удалению фишки из позиции, маркирующей эту угрозу. Это означало бы исчезновение угрозы на соответствующем элементе объекта информатизации, что противоречит логике решаемой задачи.

Указанного недостатка можно избежать, если каждую позицию, соответствующую элементу объекта информатизации, преобразовать в так называемую позицию-«ловушку», т.е. позицию, которую не может покинуть ни одна фишка (рис. 1).

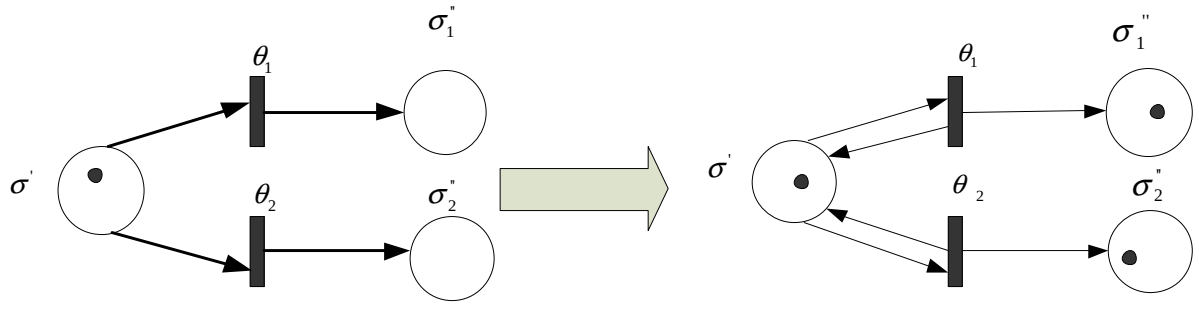

Рис. 1. Преобразование позиций в позиции-«ловушки»

После преобразования получаем сеть $\Psi_2 = \left(\Sigma, \Theta^{(1)}, h, \lambda_2, \eta_2\right)$, где обобщенные функции входов и выходов η_2 и λ_2 соответственно задаются следующим образом:

если вершина v_j, соответствующая позиции σ_j, является началом дуг $e_{ji}, e_{j2},\ldots,e_{jp}$, которые были преобразованы в переходы $\theta_{j1}, \theta_{j2},\ldots, \theta_{jp}$, то

$\eta_2(\theta_{ji}) = \sigma_j, \eta_2(\sigma_j) = \theta_{ji}\, j_i = 1,...,\mathrm{p};\ \lambda_2(\sigma_j) = \{\theta_{j1},...,\theta_{jp}\}$;

если вершина v_k, соответствующая позиции σ_k, — конец дуг $\theta_{k1}, \theta_{k2},\ldots,\theta_{kp}$, то $\lambda_2(\theta_{ki}) = \sigma_k, \lambda_2(\sigma_k) = \theta_{ki}, k_i = 1,...,\mathrm{p}; \eta_2(\sigma_k) = \{\theta_{k1},...,\theta_{kp}\}$.

Будем считать, что с каждым переходом θ ассоциируется бинарное отношение $\Re_\theta^{(1)}$ на множестве угроз информационной безопасности — «способствовать появлению».

Будем называть переход θ, которому соответствует бинарное отношение $\Re_\theta^{(1)}$, переходом, оснащенным бинарным отношением $\Re_\theta^{(1)}$.

Легко видеть, что всегда бинарные отношения $\Re_\theta^{(1)}$ обладают свойством рефлексивности, т. е. для каждой угрозы u выполняется свойство $u\Re_\theta^{(1)}u$. Другие свойства бинарного отношения проявляются в зависимости от ситуации.

Доопределим правила выполнения переходов для переходов, оснащенных бинарным отношением $\Re_\theta^{(1)}$. Будем считать, что переход θ, имеющий цвет h^i, разрешен, если в его входные позиции $\sigma' = \eta(\theta)\ \mu^j(\sigma') \rangle 0$, где h^j — цвет угрозы u_j, для которой $u_j\Re_\theta^{(1)}u_i$, т. е. в позиции σ' есть фишка, цвет которой соответствует угрозе u_j, способствующей появлению угрозы u_i.

Выполнение перехода θ, оснащенного бинарным отношением $\Re_\theta^{(1)}$, означает изменение маркировки его входной позиции σ' и выходной позиции σ'', следующим образом:

$\mu^j(\sigma') - 1 + 1 = \mu^j(\sigma')$, т. е. маркировка позиции σ' не изменяется в силу того, что эта позиция представляет собой «ловушку»;

$\mu^j(\text{г}\ddot{\text{Р}}) = \min(1,\ \text{г}\ddot{\text{К}}(\text{г}\ddot{\text{Р}}) + 1)$, $\mu^i(\sigma'') = \min(1, \mu^i(\sigma'') + 1)$.

Будем считать, что с каждым переходом θ ассоциируется бинарное отношение $\Re_\theta^{(1)}$ на множестве угроз информационной безопасности — «способствовать появлению».

2-й этап: разработка сетевой модели, учитывающей возможность устранения угроз информационной безопасности. Для предотвращения реализации угроз ИБ в соответствии с политикой информационной безопасности используются различные средства защиты, представляющие собой элементы СЗИ. В общем случае элементы СЗИ можно разделить на два типа:

предотвращающие распространение угроз ИБ от одного элемента объекта информатизации к другому;

устраняющие угрозы ИБ на самих элементах объекта информатизации.

Первоначально рассмотрим вопрос моделирования действий элементов СЗИ, осуществляющих предотвращение распространения угроз ИБ между элементами объекта информатизации. Для этого могут быть использованы так называемые сдерживающие дуги.

Каждому элементу СЗИ ставится в соответствие позиция, маркируемая фишками, цвет которых соответствует угрозам, предотвращаемым этим элементом. Сдерживающие

дуги направлены от позиций, соответствующих элементам СЗИ, к переходам, соответствующим блокируемым путям распространения угроз информационной безопасности соответствующих типов.

Правило запуска перехода в сетях со сдерживающими дугами следующее: переход является разрешенным, когда фишки того же цвета, что и цвет перехода, присутствуют во всех «обычных» входах, т.е. входах, соответствующих элементам объекта информатизации, и отсутствуют в «сдерживающих» входах, т. е. входах, соответствующих элементам СЗИ. Правило выполнения перехода не изменяется: удаляются фишки из всех его «обычных» входов. Сдерживающая дуга из позиции σ' в переход θ графически изображается маленьким кружком (а не стрелкой) у конца дуги, присоединенного к переходу.

После преобразования получаем сеть $\Psi_3 = \left(\Sigma \cup \Xi^{(1)}, \Theta^{(1)}, \Re^{(1)}, h, \lambda_3, \eta_3\right)$,

где $\Xi^{(1)}$ — множество позиций, соответствующих элементам СЗИ, препятствующим распространению угрозы ИБ; $\Re^{(1)}$ — множество бинарных отношений $\Re_\theta^{(1)}$ для всех $\theta \in \Theta^{(1)}$; обобщенные функции входов и выходов η_3 и λ_3 не изменяются для ранее ввденных переходов, соответствующих элементам объекта информатизации, т.е. $\eta_3\Big|_{\Sigma \cup \Theta} = \eta_2$, $\lambda_3\Big|_{\Sigma \cup \Theta} = \lambda_2$,

и доопределяют ранее используемые функции η_2 и λ_2 для вновь введенных позиций следующим образом:

если соответствующая элементу СЗИ позиция ξ_j, может блокировать распространение угроз, описываемых переходами θ_{j1}, θ_{j2},..., θ_{jp}, то

$\eta_3(\theta_{ji}) = \xi_j$, $j_i = 1,...,\mathrm{p}$; $\{\theta_{\mathrm{j}1}, ..., \theta_{jp}\} \in \lambda_3(\xi_\mathrm{j})$.

Обратимся к рассмотрению вопроса моделирования действий элементов СЗИ, осуществляющих устранение угроз ИБ на самих элементах объекта информатизации. Такие элементы можно моделировать с помощью введения дополнительно позиций-ловушек.

Обозначим $\Xi^{(2)}$ — множество позиций, соответствующих элементам СЗИ, устраняющим угрозы информационной безопасности на элементах объекта информатизации.

При этом будем считать, что с каждым переходом $\theta \in \Xi^{(2)}$ ассоциируется бинарное отношение $\Re_\theta^{(2)}$ на множестве угроз информационной безопасности — «способствовать устранению».

Как и ранее вновь введенные бинарные отношения $\Re_\theta^{(2)}$ обладают свойством рефлексивности, т. е. для каждой угрозы u выполняется свойство $u \Re_\theta^{(2)} u$. Другие свойства бинарного отношения проявляются в зависимости от ситуации.

Порядок выполнения переходов, оснащенных бинарными отношениями, не изменяется.

После описанного выше преобразования получаем сеть

$\Psi_4 = \left(\Sigma \cup \Xi, \Theta, h_4, \lambda_4, \eta_4\right)$,

где $\Xi = \Xi^{(1)} \cup \Xi^{(2)}$— множество позиций, соответствующих элементам СЗИ;

$\Theta = \Theta^{(1)} \cup \Theta^{(2)}$ — переходы, соответствующие процессам устранения угроз ИБ на элементах объекта информатизации;

обобщенные функции входов и выходов η_4 и λ_4 не изменяются для ранее введенных переходов, соответствующих элементам объекта информатизации, т.е.

$\eta_4\Big|_{\Sigma\cup\Xi^{(1)}\cup\Theta^{(1)}} = \eta_3$, $\lambda_4\Big|_{\Sigma\cup\Xi^{(1)}\cup\Theta^{(1)}} = \lambda_3$,

и доопределяют ранее используемые функции η_2 и λ_2 для вновь введенных позиций следующим образом: если соответствующая элементу СЗИ позиция ξ_j, может устранять угрозы на элементе объекта информатизации, которому соответствует позиция σ_i с помощью перехода θ, то

$\eta_4(\theta) = \{\xi_j, \sigma_i\}$; $\lambda_4(\theta) = \xi_j; \eta_4(\xi_j) = \lambda_4(\xi_j) = \theta; \theta \in \lambda_4(\sigma_i)$;

функция раскраски переходов не изменяется для ранее введенных переходов, т.е. $h_4\Big|_{\Theta^{(1)}} = h$, и доопределяется для переходов множества $\Theta^{(2)}$ в соответствии с функциональными возможностями элемента СЗИ.

3-й этап: разработка сетевой модели, учитывающей динамику распространения и устранения угроз информационной безопасности. Во вновь полученной сети Ψ_4 позиции, соответствующие элементам объекта информатизации, уже перестают быть ловушками, так как они могут терять фишки после выполнения переходов из множества $\Theta^{(2)}$, соответствующих устранению угрозы. Кроме того, возникает возможность появления конфликтов.

Каждый переход соответствует определенному процессу передачи или устранения угрозы ИБ, эти процессы имеют определенную продолжительность.

Перейдем к рассмотрению временной сети, в которой заданы времена выполнения переходов, т. е. определена функция $T : \Theta \to [0,+\infty)$, ставящая в соответствие каждому переходу $\theta \in \Theta$ его длительность выполнения $t \geq 0$.

Для предотвращения конфликтов введем правило выбора последовательности выполнения выходных переходов для каждой позиции, моделирующей элемент объекта информатизации, определяемое бинарным отношением $\Im$ — «выполняться ранее».

Пусть $\theta_1, \theta_2, \ldots, \theta_s$ — выходные переходы позиции σ, активные в данной момент времени $t_1, t_2, \ldots, t_s$ — длительность выполнения переходов.

Последовательность выполнения переходов определена на основе анализа значений в соответствии со следующим условием:

если $t_i < t_j$, то $\theta_i \Im \theta_j$. Тем самым определена сеть $\Psi_5 = (\Sigma \cup \Xi, \Theta, \Re, \Im, T, h_5, \lambda_5, \eta_5)$, где $h_5 \equiv h_4$, $\lambda_5 \equiv \lambda_4$, $\eta_5 \equiv \eta_4$.

Разработана модель распространения и устранения угроз ИБ на объекте информатизации ОВД, позволяющая учесть возможность возникновения новых типов угроз на отдельных элементах объекта.

Численный метод реализации сетевой модели. Для численного представления процессов разработанной выше сети будем использовать матричное представление. Обозначим:

$D^- = (d_{ij}^-)$ — матрицу входов в переходы, определяемую по правилу:

$$d_{jk}^- = \begin{cases} 1, \textit{ если позиция } \sigma_j \textit{ является входом для перехода } \theta_k \\ 0, \textit{ если иначе;} \end{cases}$$

$D^+ = (d_{ij}^+)$ — матрицу выходов из переходов, определяемую по правилу:

$$d_{jk}^+ = \begin{cases} 1, \textit{если позиция } \sigma_j \textit{ является выходом для перехода } \theta_k, \\ 0, \textit{ если иначе.} \end{cases}$$

$D = D^+ - D^-$ составная матрица изменений.

Для наглядности строки, соответствующие переходам разного цвета, разделяются двойной линией.

X — матрица разрешенных переходов, т.е. таких переходов θ_i, для которых в маркировке μ выполняется следующее условие: $\mu \geq X_i \otimes D^-$, где $\otimes$ — матричная операция логического умножения, которая определяется по следующему правилу:

если $A = (a_{ij})$, где $i = 1,\ldots,n$, $j = 1,\ldots,m$, $B = (b_{jk})$, где $j = 1,\ldots,m$, $k = 1,\ldots,l$ — логические матрицы, то $C = A \otimes B$ — логическая матрица, такая, что $c_{ik} = \bigvee_{j=1}^{m} a_{ij} \wedge b_{jk}$.

$\Re$ — матрица соответствующих разрешенным переходам бинарных отношений. Маркировка μ задается отдельно для каждого цвета фишек.

Для пояснения способа формирования этих матриц рассмотрим пример сети, содержащей переходы 3 цветов (рис. 2).

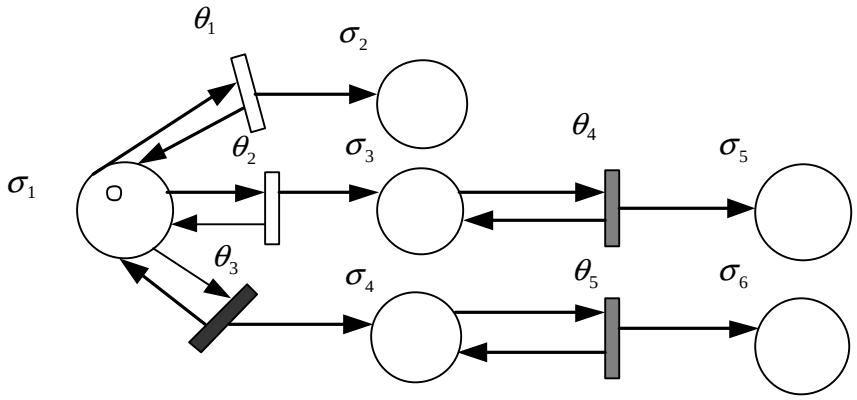

Рис. 2. Пример трехцветной сети

Матрицы, описывающие эту сеть, имеют следующий вид:

$$D^- = \left(\begin{array}{cccccc} 1&0&0&0&0&0 \\ 1&0&0&0&0&0 \\ \hline\hline 1&0&0&0&0&0 \\ \hline\hline 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \end{array}\right),\ D^+ = \left(\begin{array}{cccccc} 1&1&0&0&0&0 \\ 1&0&1&0&0&0 \\ \hline\hline 1&0&0&1&0&0 \\ \hline\hline 0&0&1&0&1&0 \\ 0&0&0&1&0&1 \end{array}\right),\ D = \left(\begin{array}{cccccc} 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ \hline\hline 0&0&0&1&0&0 \\ \hline\hline 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{array}\right),$$

$$X_1 = \left(\begin{array}{ccc||c||cc} 1&1&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{array}\right),\ \Re_1 = \left(\begin{array}{ccc||c||cc} 0&0&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \end{array}\right),\ \mu = \left(\begin{array}{cccccc} 1&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{array}\right).$$

После выполнения разрешенных переходов θ_1, θ_2 сеть получает маркировку μ^1, в соответствии с которой позиции σ_2, σ_3 получат не только белую, но и серую и черную фишки (рис. 3).

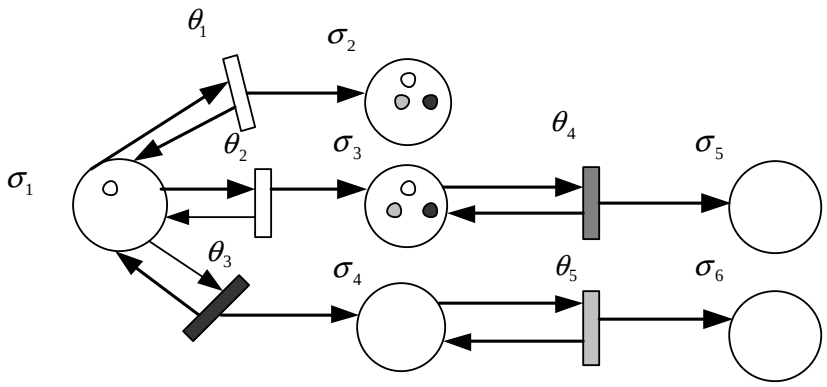

Рис. 3. Сеть после выполнения разрешенных переходов

Достижимая маркировка сети определяется по формуле: $\mu^1 = \mu \vee (x \vee \Re) \otimes \mathrm{D}$, которая развернуто представляется следующим образом:

$$\mu^1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \vee \left(\left(\begin{array}{cc|c|cc} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \vee \left(\begin{array}{cc|c|cc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{array} \right) \right) \otimes \left(\begin{array}{cccccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline\hline 0 & 0 & 0 & 1 & 0 & 0 \\ \hline\hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right) =$$

$$= \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Заключение. Разработанные математическая модель и численный метод позволяют имитировать процесс распространения и устранения угроз информационной безопасности на объектах информатизации органов внутренних дел, что может быть использовано при проектировании или модификации систем защиты информации этих объектов.

ЛИТЕРАТУРА

1. Герасименко В.А., Малюк А.А. Основы защиты информации: учебник для высших учебных заведений Министерства общего и профессионального образования РФ. — М.: МИФИ, 1997. — 538 с.

2. Меньших В.В., Лунев Ю.С. Моделирование действий дестабилизирующих факторов на распределенные информационные системы с помощью аппарата сетей Петри // Системы управления и информационные технологии. — 2008. — № 1(31). — С. 71—75.

3. Меньших В.В., Петрова Е.В. Применение методов теории автоматов для моделирования информационных процессов // Вестник Воронежского института МВД России. — 2009. — № 1. — С. 121—130.

4. Меньших В.В., Петрова Е.В. Синтез автоматной модели функционирования информационной системы в условиях воздействия угроз информационной безопасности // Инженерная физика. — 2010. — № 3. — С. 43—44.

5. Меньших В.В., Толстых О.В. Моделирование возникновения угроз информационной безопасности на объекте информатизации // Информация и безопасность. — 2011. — Вып. 1. — С. 117—120.

6. Кудрявцев В. Б., Алешин С. В., Подколозин А.С. Введение в теорию автоматов. — М.: Наука, 1985. — 320 с.

7. Питерсон Дж. Теория сетей Петри и моделирование систем. — М.: Мир, 1984. — 264 с.

8. Логико-лингвистические модели в военных системных исследованиях / Н.Г. Бублик [и др.]; под ред. Е.А. Евстигнеева. — М.: Военное издательство, 1988. — 232 с.