УДК 004.45, 004.89, 681.3

ПРЕДСТАВЛЕНИЕ ЗНАНИЙ ОБ УПРАВЛЕНИИ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ НЕЧЕТКИХ ВРЕМЕННЫХ РАСКРАШЕННЫХ СЕТЕЙ ПЕТРИ

С. В. Гладыш

Анотація: Досліджено проблему інтелектуального керування інцидентами інформаційної безпеки. Вирішується задача подання знань в даній системі. Проведен аналіз невизначеності, що виникає, накладаючи вимоги на вибір мови подання знань. Розглянуто формалізм мереж Петрі, і на його базі запропоновано клас нечітких часових розфарбованих мереж Петрі. Показано можливість його використання в рамках інтелектуальної системи підтримки прийняття рішень щодо керування інцидентами інформаційної безпеки.

Аннотация: Исследована проблема интеллектуального управления инцидетами информационной безопасности. Решается задача представления знаний в даннной системе. Проведен анализ возникающей неопределенности, накладывающий требования на выбор языка представления знаний. Рассмотрен формализм сетей Петри, и на его базе предложен подкласс нечетких временных раскрашенных сетей Петри. Показана возможность его использования в рамках интеллектуальной системы поддержки принятия решений по управлению инцидентами информационной безопасности.

Abstract: The research is devoted to the problem of intelligence management on information security incidents. The task of knowledge representation in the given system is being solved. The uncertainness, which takes place, is determine the requirements on a choice of a knowledge representation language. Formalism of Petri nets is considered, and on its basis a subclass of fuzzy timed colored Petri nets is proposed. The given subclass in use is presented in intelligence decision making support system on information security incidents management..

Ключові слова: інформаційна безпека, інцидент, нечітка логіка, прийняття рішень, мережі Петрі.

Введение

Проблема представления знаний об инцидентах информационной безопасности (ИБ) возникает при автоматзации и интеллектуализации процесса управления инцидентами и связана с аккумулированием, систематизацией накопленного опыта [1] в области реагирования, обработки и расследования, обобщения существующей нормативно-методологической базы [2], построения соответствующей интеллектуальной системы поддержки принятия решений (ИСППР) [3 - 6].

Задача представления, описания и обработки нечетких представлений, наблюдений, суждений и решений, связанных с инцидентами ИБ и управлением ими с целью эффективного их использования в ИСППР обусловлена необходимость принятия решений в условиях ограниченных ресурсов, неопределенности различного происхождения, неточности, субъективности [7], нечеткости при управлении инцидентами ИБ в большинстве случаев накладывает ограничения на применимость как “четких”, так в некоторых случаях и нечетких математических подходов [8].

В исследованиях [9 – 11] начата разработка и обоснование подхода к нечеткому моделированию и представлению знаний для решения научных и научно-практических задач ИБ, основанного на использовании различных классов и обобщений сетей Петри (СП). В частности разработаны модели распределения ресурсов ИБ в телекоммуникационных системах [9], построеныые на нечетких СП с частичным использованием нечетких нейронных сетей [10, 11].

Однако, как показывает поиск в Интернете [1, 12] применительно к управлению инцидентами ИБ вопрос представления знаний посредством нечетких СП не ставился и в настоящее время не решен.

Целью настоящего исследования является разработка, обоснование и использование подкласса нечетких временных раскрашенных СП в качестве языка представления знаний (ЯПЗ) в ИСППР по управлению инцидентами ИБ.

Задачи исследования: определить требования и обосновать выбор ЯПЗ для управления инцидентами ИБ; предложить математически формализованную структуру адекватного подкласса СП; рассмотреть возможность использования данного подкласса путем задания общей структуры базы знаний ИСППР для управления инцидентами ИБ.

Определение требований к языку представления знаний об управлении инцидентами ИБ

Представления экспертов [13] или членов группы реагирования на инциденты ИБ (CSIRT) [14, 15] об инцидентах ИБ и управлении ими являются по самой своей природе ***нечеткими***. Для эксперта по ИБ очевидны, понятны и естественны понятия: "*высоко критичная* инфокомуникационная инфраструктура", " *серьезный* инцидент", " *слабая* угроза", " *высокая* производительность", " *большая* вероятность взлома", *“ небольшое* количество ресурса” и т.п. Нечеткий вывод из нечетких условных утверждений типа:

«Если система “*высоко критичная”* и *“средняя”* угроза, то система защиты должна выделить “*умеренно высокое”* количество ресурса», вполне характерен для деятельности CSIRT. Это приводит к необходимости разработки адекватных подходов к принятию решений и обработке информации об упралении инцидентами ИБ [3, 4].

Выделим следующие факторы, которые оказывают влияние на установление требований к ЯПЗ:

- не все цели и критерии управления инцидентами ИБ могут быть представлены в виде количественных соотношений;
- между некоторыми параметрами, оказывающими влияние на процесс управления инцидентами ИБ, не удается или очень сложно установить точные количественные зависимости;
- процесс управления инцидентами ИБ является многошаговым и многоэтапным, а содержание каждого шага и этапа не всегда может быть заранее однозначно определено, существующие описания и представления слишком громоздки;
- инфокоммуникационные объекты и процессы развиваются во времени, что требует изменений законов управления инцидентами ИБ, а сама динамика указанных процессов неясна или представлена нечетко.

Кроме того CSIRT приходится функционировать в условиях ограничений на временные, информационные, телекоммуникационные, вычислительные, человеческие и материальные ресурсы [9, 14, 15]. При этом некоторые характеристики инцидентов ИБ недоступны для количественных оценок и могут быть представлены только лингвистически [13].

Рассмотрим некоторые общие представления о неопределенности, нечеткости, неточности при управлении инцидентами ИБ, а затем определим адекватные ЯПЗ (табл..1).

Таблица 1. Виды неопределенности и соответствующие им ЯПЗ об управлении инцидентами ИБ

Вид неопределенности	**Проявление неопределенности**	**ЯПЗ**
Стохастическая неопределенность возникновения инцидента ИБ	Событие, состоящее в возникновении инцидента ИБ, обусловлено случайностью	Статистика и теории вероятностей [8], стохастические СП [17]
Нечеткость восприятия инцидента ИБ	Субъективность или индивидуальность восприятия инцидента ИБ человеком	Субъективная логика [7] и лингвистическая переменная [13]
Нечеткость суждения об инциденте ИБ	Нечеткость или неопределенность в процессах мышления или умозаключения а) нечеткое или неточное заключение об инциденте ИБ; б) неясность вследствие сложности и (или) многообразия выводов об инциденте ИБ	Нечеткая логика, нечеткие продукции, нечеткие СП [9 – 11, 16, 23]. Когнитивное моделирование, экспертные методы [13]
Нечеткость или неопределенность, сопутствующая высказываниям об инциденте ИБ на естественном языке	а) нечеткость описания или представления инцидента ИБ; б) неопределенность инцидента ИБ, связанная со сложностью и многообразием семантик и структур естественных языков	Лингвистическая переменная [13]. Модели семантики информации, нечеткие СП [9 – 11, 16, 23]
Неопределенность идентификации сигнатур инцидента ИБ	Распознавание образов сигнатур инцидентов ИБ	Инскусственные нейронные сети [10, 11, 16, 23]
Неопределенность из-за структурной сложности инцидента ИБ	Многообразие информации об инциденте ИБ	Нечеткие СП [9 – 11, 16, 23]

Вследствие наличия качественной (нечисловой) информации, связанной с управлением инцидентами ИБ, можно предложить следующие механизмы проверки и подтверждения адекватности нечетких моделей [16]:

- использование обучающих данных об инцидентах ИБ: эффективность модели определяется количественно, рассматриваются те же самые данные, которые используются в реальной системе;
- использование проверочных данных об инцидентах ИБ: качество модели оценивается путем использования данных, которые отличаются от используемых первоначально в разработке модели.

На сегодня научный и научно-практический интерес [1] представляет управление инцидентами ИБ в ***распределенных*** инфокоммуникационных системах. При этом процессы управления инцидентами носят параллельный распределенный характер и могут быть выражены в терминах: «условие - действие». Как известно [12, 19, 20], для указанного типа процессов наиболее адекватным математическим языком являются СП.

Необходимо также учесть, что при реагировании и обработке инцидентов огромную роль играет фактор ***времени***. Следовательно, ЯПЗ должен давать возможность отображать логико-временные характеристики рассматриваемых процессов. Данному требованию удовлетворяют временные СП [12].

Современные инфокоммуникационные системы, применительно к которым может рассматриваться проблема управления инцидентами ИБ, являются структурно сложными и большемасштабными гетерогенными системами [9]. Модели таких систем и представление знаний о них должны иметь огромную ***размерность***, что создает вычислительные трудности. Одним из способов понижения размерности модели для СП является внесение функции ***цвета*** в маркировку, т.е.

определение «цветных» маркеров. При этом под термином «цвет» маркера имеется в виду самая разная природа сложных маркеров-объектов, маркеров-предикатов, маркеров-процедур и т.п [12, 18]. Сети такого типа получили название раскрашенных СП.

Поэтому, учитывая и обосновываясь вышесказанными соображениями, автором в настоящем исследовании для решения задачи представления знаний об управлении инцидентами ИБ выбран формализм ***нечетких временных раскрашенных СП***.

Определение базовых положений теории сетей Петри, необходимых для представления знаний по управлению инцидентами ИБ

СП относятся к числу наиболее важных и распространенных математических моделей в области обработки информации. Разработан и утвержден специальный международный стандарт ISO [18], определяющий общие принципы и структуру высокоуровневых СП. Исследованию и использованию СП посвящена обширная библиография, одним из наиболее современных и полных отображений которой является [12]. Среди фундаментальных работ в области СП, которые давно доступны отечественному исследователю, отметим [19 - 21].

Кратко охарактеризуем основные моменты теории СП, которые необходимы для определения нечетких СП, и будут использоваться в настоящем исследовании.

Визуально СП представляет собой ориентированный граф специального вида (рис.1) с определенными правилами, которые определяют динамику процесса его функционирования.

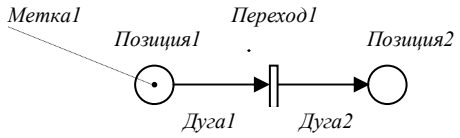

Рисунок 1 – Графическое представление сети Петри

Граф СП имеет 2 типа вершин: *позиции* (places) и *переходы* (transitions), а также ребра – направленные *дуги* (arcs). Внутри позиций имеются *маркеры* (markers), определяемые начальной маркировкой СП, которые на рис.1 обозначены точками как самый простой случай. В случае высокоуровневых СП маркеры могут иметь более сложную структуру (раскрашенные маркеры, маркеры-объекты [18, 9 - 11], маркеры-агенты [17], маркеры-ресурсы [9 - 11] и др.).

Правила функционирования СП формализуют динамические отношения между позициями, содержащими маркеры, путем воспроизведения условий срабатывания переходов, через которые позиции связываются друг с другом. Срабатывание перехода, приводит к изменению разметки: из каждой входной позиции удаляется количество меток равное кратности исходящих дуг, а в выходные позиции добавляется по числу меток равных кратности входящих дуг. Переход сработает если число меток во входной позиции больше или равно кратности дуг, выходящих из данной позиции. Если кратность всех дуг не превышает 1, то СП называется *ординарной*. Если количество маркеров в любой позиции при любой достижимой разметке не превышает 1, то СП называется *безопасной*.

Кроме того СП может быть формализована и исследована в аналитическом (алгебраическом) представлении. Наличие строго определенных, теоретически обоснованных графовой и алитической формы СП позволяет говорить о *специальном математическом языке – языке СП* [20].

Аналитическое определение обобщенной маркированной СП (PN) – упорядоченная пятерка:

$$PN = \left\langle P, \quad T, \quad I, \quad O, \quad m^0, \quad \Re \right\rangle, \qquad (1)$$

где $P = \{p_1, \quad p_2, \ldots, p_n\}$ - множество позиций;

$T = \{t_1, \quad t_2, \ldots, t_u\}$ - множество переходов;

$I \quad : \quad P \times T \to \aleph_0$ - входная функция переходов;

$O \quad : \quad T \times P \to \aleph_0$ - выходная функция переходов;

$m^0 = \left(m_1^0, \quad \ldots, \quad m_n^0\right)$ - вектор начальной маркировки;

$m_i^0 \in \aleph_0 \quad \left(\forall i \in \{1, 2, \ldots, n\}\right)$ - компонент вектора начальной маркировки СП, соответствующий позиции $p_i \in P$;

$\aleph_0 = \{0, 1, 2, 3, \ldots\}$ - множество целых неотрицательных чисел;

$\Re$ - набор правил функционорования СП.

Для ординарной СП (PN_{Ord}) соответственно: $I : P \times T \to \{0, \quad 1\}$; $O : T \times P \to \{0, \quad 1\}$.

Первые 4 компонента, которые задают структуру СП, могут быть выделены как $N = (P, \quad T, \quad I, \quad O)$. Тогда СП записывается в виде:

$$PN = \langle N, \quad m^0, \quad \Re \rangle. \qquad (2)$$

Динамика СП подчиняется правилам:

$\Re_1$: *определение текущего состояния СП*. Любое состояние СП определяется некоторой его маркировкой $m = (m_1, \quad \ldots, \quad m_n)$.

$\Re_2$: *активность перехода*. Переход $t_j \in T$ активен при маркировке $m^k = (m_1^k, \quad \ldots, \quad m_n^k)$ если выполнено условие:

$$m_i^k \geq I(p_i, \quad t_j), \quad \forall p_i \in P. \qquad (3)$$

$\Re_3$: *срабатывание перехода*. Если переход $t_j \in T$ активен при маркировке $m^k = (m_1^k, \quad \ldots, \quad m_n^k)$, то срабатывание данного перехода приводит к новой маркировке сети $m^{k+1} = (m_1^{k+1}, \quad \ldots, \quad m_n^{k+1})$:

$$m_i^{k+1} = m_i^k + O(t_j, p_i) - I(p_i, t_j), \quad \forall p_i \in P. \qquad (4)$$

Помимо базового классического формализма (1) - (4) на сегодня уже разработан и продолжает развиваться целый ряд разновидностей и обобщений СП, предназначенных для моделирования и анализа различных структурных, функциональных, процессуальных, временных, вероятностных, когнитивных и др. аспектов изучаемых динамических дискретных систем, параллельных распределенных явлений и логико-временных процессов [12].

Для раскрашенных СП (CPN – Colored Petri Nets) формализм обобщенной маркированной СП расширяется за счет включения в рассмотрение маркеров различного «цвета», с соответствующим видоизменением правил СП:

$$CPN = \langle N, \quad m^0, \quad C, \quad \Re_C \rangle. \qquad (5)$$

где $c(m_i) \in C$ - функция, соответствующая цвету (типу) метки в позиции $p_i \in P$.

Для временных СП к формализму обобщенной маркированной СП добавляются 2 новых компонента, которые изменяют правила функционирования с учетом логико-временных особенностей:

$$PN_T = \langle N, \quad m^0, \quad z, \quad s, \quad \Re_T \rangle, \qquad (6)$$

где $z = (z_1, ..., z_n)$ - вектор временных задержек маркеров в позициях СП;

$s = (s_1, ..., s_n)$ - вектор вектор времен срабатывания разрешенных переходов СП;

$\Re_T$ - набор правил функционорования СП с учетом логико-временных характеристик.

Включение *нечеткости* в различные разновидности и обобщения СП также может быть осуществлено различными способами по каждому из компонентов исходного формализма обобщенной маркированной СП. В работах [22, 23] рассмотрено несколько основных типов нечетких СП (FPN – Fuzzy Petri Net). Имеются примеры [9 – 11, 22] использования FPN для представления правил нечетких продукций. Это позволяет говорить об ***FPN*** как о ***множестве языков представления знаний***.

Разработка подкласса нечетких временных раскрашенных сетей Петри как языка представления знаний по управлению инцидентами ИБ

Исходя из требований к ЯПЗ об управлении инцидентами ИБ, которые были определены в разделе 1 настоящей статьи ИБ, предлагается разработать и использовать в дальнейшем специальный подкласс $\mathbf{FCPN_{SecOrdT}}$ (Secure Ordinary Timed Fuzzy Colored Petri Net), основанный на введении нечеткости в *начальную маркировку* и *правила срабатывания переходов* формализма безопасных

ординарных временных раскрашенных СП. Графическая структура предложенного подкласса $FCPN_{SecOrdT}$ идентична графической структуре ординарной СП (PN_{Ord}) и изображается ориентированным двудольным графом.

Однако учет требований к управлению инцидентами ИБ, аналитическая структура, особенности введения нечеткости и специальные правила функционирования будут ***отличать*** разрабатываемый подкласс $FCPN_{SecOrdT}$ от существующих. Представим данный подкласс аналитически:

$$FCPN_{SecOrdT} = \left\langle N_{Ord},\quad \widetilde{m}_C^0,\quad \widetilde{f}_c,\quad \widetilde{\lambda}_c,\quad C,\quad z_c,\quad s_c,\quad \widetilde{\Re}_{CT} \right\rangle, \qquad (7)$$

где $N_{SecOrd} = \left(P,\quad T,\quad I,\quad O\right)$ - структура безопасной ординарной СП;

$P = \left\{p_1,\quad p_2, \ldots, p_n\right\}$ - множество позиций;

$T = \left\{t_1,\quad t_2, \ldots, t_u\right\}$ - множество переходов;

$I : P \times T \to \left\{0,\quad 1\right\}$ - входная функция переходов;

$O : T \times P \to \left\{0,\quad 1\right\}$ - выходная функция переходов;

$\widetilde{m}_C^0 = \left(m_{11}^0, ..., m_{1n}^0;\quad m_{21}^0, \ldots, m_{2n}^0;\quad m_{C1}^0, ..., m_{Cn}^0\right)$ - матрица начальной маркировки, каждый элемент которой является нечеткой (L-R)-величиной, опреляющей нечеткое наличие в позиции $p_i \in P$ одного маркера соответственно для каждого из цветов $c \in C$;

m_{ci} $\left(\forall i \in \left\{1, 2, \ldots, n\right\},\quad \forall c \in \left\{1, ..., C\right\}\right)$ - элемент маркировки, соответствующий нечеткому наличию в позиции $p_i \in P$ одного маркера данного цвета $c \in C$;

$\widetilde{f}_C = \left(f_{11}, ..., f_{1u};\quad f_{21}, \ldots, f_{2u};\quad f_{C1}, ..., f_{Cu}\right)$ - матрица нечетких (L-R)-величин, определяющих нечеткое срабатывание переходов соответственно для маркеров каждого из цветов $c \in C$;

$\widetilde{\lambda}_C = \left(\lambda_{11}, ..., \lambda_{1u};\quad \lambda_{21}, \ldots, \lambda_{2u};\quad \lambda_{C1}, ..., \lambda_{Cu}\right)$ - матрица нечетких (L-R)-величин, определяющих пороги срабатывания нечетких переходов соответственно для маркеров каждого из цветов $c \in C$;

$c(m_i) \in C$ - функция, соответствующая цвету маркера $c \in C$ в позиции $p_i \in P$;

$z_C = \left(z_{11}, ..., z_{1n};\quad z_{21}, \ldots, z_{2n};\quad z_{C1}, ..., z_{Cn}\right)$ - матрица временных задержек маркеров соответственно для маркеров каждого из цветов $c \in C$ в позициях $FCPN_{SecOrdT}$;

$s_C = \left(s_{11}, ..., s_{1n};\quad s_{21}, \ldots, s_{2n};\quad s_{C1}, ..., s_{Cn}\right)$ - матрица времен срабатывания разрешенных переходов $FCPN_{SecOrdT}$ соответственно для маркеров каждого из цветов $c \in C$;

$\widetilde{\Re}_{CT}$ - набор правил функционорования $FCPN_{SecOrdT}$, модификация которых отражает специфику введенной нечеткости, цветных маркеров и логико-временных характеристик:

$\widetilde{\Re}_{CT1}$: ***определение текущего состояния на момент*** τ. Любое состояние $FCPN_{SecOrdT}$ в любой момент времени τ определяется нечеткой матрицей маркировки, элементы которой интерпретируются как термы функции принадлежности нечеткого наличия одного маркера в соответствующих позициях относительно времени, отсчитываемого от момента запуска данной $FCPN_{SecOrdT}$ соответственно для маркеров каждого из цветов $c \in C$.

$\widetilde{\Re}_{CT2}$: ***активность перехода на момент*** τ. Переход $t_j \in T$ активен для маркеров определенного цвета $c \in C$ при некоторой доступной маркировке $\widetilde{m}_C^k$ если выполнено условие:

$$\min_{\left(i \in \left\{1, 2, ..., n\right\} \wedge I\left(p_i, t_j\right) \rangle\, 0\right)} \left\{m_{ci}^k\right\} \geq \lambda_{cj}, \qquad (8)$$

т.е. во всех входных позициях данного перехода на момент времени τ должны быть доступные маркеры, представленные отличными от нуля нечеткими величинами, причем минимальная из них должна быть не меньше порога срабатывания данного перехода.

$\widetilde{\Re}_{CT3}$: ***срабатывание перехода за время*** s_{cj} . Если переход $t_j \in T$ активен при некоторой доступной маркировке $\widetilde{m}_C^k$ (для него выполнено условие (8)), то срабатывание данного перехода за время $s_{cj} \in s_C$ приводит к новой маркировке сети m_C^{k+1}, элементы которой определяются так:
для каждой из входных позиций $p_i \in P$, для которых $I(p_i, t_j) \rangle 0$:

$$m_{ci}^{k+1} = 0, \quad (\forall p_i \in P) \wedge (I(p_i, t_j) \rangle 0); \tag{9}$$

для каждой из выходных позиций $p_l \in P$, для которых $O(t_j, p_l) \rangle 0$:

$$m_{cl}^{k+1} = \max\left(m_{cl}^k, \min_{(i \in \{1,2,\ldots,n\}) \wedge (I(p_i,t_j) \rangle 0)} \left(m_{ci}^k, f_{cj} \right) \right) \quad (\forall p_l \in P) \wedge (O(t_j, p_l) \rangle 0). \tag{10}$$

Если некоторые из позиций $p_l \in P$ являются одновременно входными и выходными для активного перехода $t_j \in T$, то для них элементы маркировки рассчитываются последовательно, сначала по (9), затем – по (10).

$\widetilde{\Re}_{CT4}$ - ***задержка маркеров в позициях на время*** z_{cl}. После нечеткого срабатывания активного перехода (правило $\widetilde{\Re}_{CT3}$) маркеры в выходных позициях для новой маркировки m_C^{k+1} не являются мгновенно доступными, т.к. на них начинают действовать временные задержки в соответствующих выходных позициях сработавшего перехода, определяемые матрицей z_C. Соответствующие маркеры становятся доступными только после временных задержек.

Введенную в маркировку и условия срабатывания переходов $FCPN_{SecOrdT}$ нечеткость мы для облегчения вычислительных аспектов условились представлять в виде (L-R)-нечетких величин. Данное представление можно конкретизировать, например, треугольными нечеткими числами, тогда:

$$\begin{aligned} m_{ci} &= \left\langle a_{ci}^m, \alpha_{ci}^m, \beta_{ci}^m \right\rangle \quad (\forall i \in \{1,2,\ldots,n\}, \quad \forall c \in \{1,\ldots,C\}); \\ f_{cj} &= \left\langle a_{cj}^f, \alpha_{cj}^f, \beta_{cj}^f \right\rangle \quad (\forall j \in \{1,2,\ldots,u\}, \quad \forall c \in \{1,\ldots,C\}); \\ \lambda_{cj} &= \left\langle a_{cj}^\lambda, \alpha_{cj}^\lambda, \beta_{cj}^\lambda \right\rangle \quad (\forall j \in \{1,2,\ldots,u\}, \quad \forall c \in \{1,\ldots,C\}). \end{aligned} \tag{11}$$

Структура нечеткой сетевой базы знаний по управлению инцидентами ИБ

Проектируемая база знаний ИСППР по управлению инцидентами ИБ должна состоять из накопленного статистически обработанного материала по фактам зарегистрированных инцидентов ИБ с извлечением их сигнатур, а также автоформализованной экспертной информации, необходимой для поддержки принятия решений по реагированию, обработке, расследованию инцидента, выбору превентивных корректирующих мер (рис. 2).

Принятие решений относительно управления инцидентами ИБ выполняется с помощью нечетких правил продукций. Каждое правило базируется на некоторой совокупности элементов $FCPN_{SecOrdT}$. С помощью правил функционирования СП $\widetilde{\Re}$ (правил решения) проводится частичное упорядочение (ранжирование) точек пространства входных показателей (смена нечетких маркировок за счет срабатывания нечетких переходов).

В $FCPN_{SecOrdT}$ для интерпретации маркеров в позициях можно использовать понятие нечеткой истинности высказывания. Поскольку значение истинности высказывания не становится равным нулю для высказываний-антецедентов в левой части правил продукций после их выполнения, то для представления правил нечетких продукций с помощью разработанного класса $FCPN_{SecOrdT}$ модифицируем правило $\widetilde{\Re}_{CT3}$. При расчете компонентов матрицы новой маркировки m_C^{k+1} будет использована единая формула (10).

Будем использовать следующую интерпретацию позиций и переходов: правило $\Re_j : if\ Ant_i\ then\ Con_l$ будем представлять в виде некоторого перехода $t_j \in T$ $FCPN_{SecOrdT}$, при этом

антецеденту Ant_i правила будет соответствовать входная позиция $p_i \in P$ данного перехода, а консеквенту Con_l - выходная позиция $p_l \in P$. Роль начальной маркировки m_C^0 будет играть входной вектор *x*, который будет расширен до матрицы за счет увеличения размерности путем учета цвета маркеров.

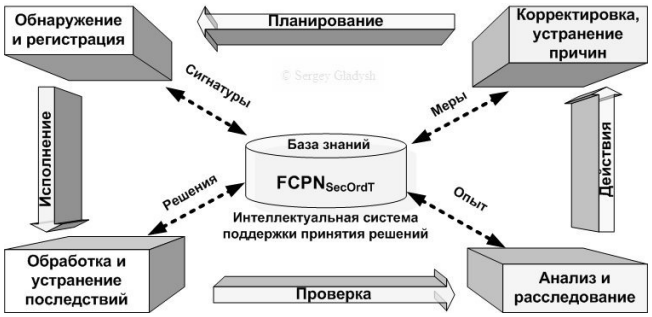

Рисунок 2 – Функциональная схема ИСППР по управлению инцидентами ИБ

Таким образом, $FCPN_{SecOrdT}$ позволяет наглядно отображать и осуществлять нечеткий вывод по правилам нечетких продукций, учитывая при этом распределенно-параллельный характер, неопределенность и логико-временные характеристики процессов управления инцидентами ИБ.

Выводы

Научным результатом настоящего исследования является новый методологический подход к решению проблемы управления инцидентами ИБ, основанный на применении ИСППР, где в качестве ЯПЗ используется разработанный в данной статье подкласс $FCPN_{SecOrdT}$.

Формальному определению ЯПЗ предшествовало определение и обоснование требований к нему применительно к специфике изучаемых процессов и явлений ИБ. Для этого была проведена классификация видов неопределенности, имеющих место при возникновении и управлении инцидентами ИБ с последующим указанием адекватных ЯПЗ. Обосновываясь установленными требованиями было проведено обобщение и расширение классического формализма СП путем разработки специального подкласса $FCPN_{SecOrdT}$, который позволяет учитывать распределенность, параллельность, нечеткость и логико временные характеристики процессов управления инцидентами ИБ. На основе полученного решения возможна практическая реализация базы знаний ИСППР для управления инцидентами ИБ. Направлениями дальнейшего исследования является конкретизация разработанной методики и аппробирование ее на примерах моделирования конкретных инцидентов ИБ.

Список литературы

1. Computer Emergency Response Team - Coordination Center: http://www.cert.org/
2. *Гладиш С. В., Кононович В. Г., Тардаскін М. Ф.* Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2007. - № 15.
3. *Gladysh S.* Decision support system on telecommunications security incidents response and handling // Збірник тез доповідей першої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації», Вінниця: ВНТУ, 2007. – с. 65 – 66.
4. *Гладиш С.В.* Інтелектуальна система керування інцидентами інформаційної безпеки телекомунікаційних мереж // Матеріали міжнародної науково-практичної конференції «Інформаційні технології та інформаційна безпека в науці, техниці та освіті», Севастопіль, СевНТУ, 2007. – с. 53 - 57.
5. *Гладыш С. В.* Модель нечеткой экспертной системы поддержки принятия решений по распределению ресурсов информационной безопасности // Сборник материалов X Юбилейного международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», Харьков: ХНУРЭ, 2006. – с. 459.
6. *Гладыш С. В.* Представление знаний в экспертной системе поддержки принятия решений по распределению ресурсов информационной безопасности информационно-телекоммуникационных сетей // Сборник докладов и тезисов IV Международного молодежного форума «Информационные технологии и кибернетика», Днепропетровск: УГХТУ, 2006. – с. 19 – 21.
7. *Потій О.В., Лєншин О.В.* Методика визначення думок експертів відносно зрілості безпеки інформації з використанням математичного апарату суб’єктивної логіки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2004. - вип. 9. - с. 38 - 47.

8. *Доценко С. М., Зайчиков А. А., Малыш В. Н.*. Повышение объективности исходных данных как альтернатива методу нечеткой логики при оценке риска информационной безопасности // Защита информации. Конфидент.- 2004. - №5.- с. 15 - 25.
9. *Гладыш С. В.* Использование нечетких сетей Петри для построения модели распределения ресурсов информационной безопасности информационно-телекоммуникационных сетей // Захист інформації. – 2007. - №1.
10. *Гладыш С. В.* Модель распределения ресурсов информационной безопасности в телекоммуникационных системах на базе нейро-фаззи сети Петри // Інформаційні технології та комп’ютерна інженерія. – 2007. - вип. 1 (8). – с. 218 – 224.
11. *Гладыш С. В.* Построение нейро-фаззи сети Петри, моделирующей динамическое распределение ресурсов информационной безопасности в информационно-телекоммуникационных системах // Збірник матеріалів V Міжнародної науково-технічної конференції «Інтернет – Освіта –Наука – 2006», Вінниця: ВНТУ, 2006. – с. 446 – 449.
12. http://www.informatik.uni-hamburg.de/TGI/PetriNets
13. *Гладыш С. В.* Организационно-методические аспекты экспертной оценки информационной безопасности телекоммуникационных систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-2006. - вип. 12. – с. 178 – 188.
14. *Гладиш С. В., Кононович В. Г., Тардаскін М. Ф.* Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування «Зв’язок». – 2007. - № 8.
15. *Gladysh S.* Distribution of responsibility on telecommunication incidents in Ukraine // Матеріали III Міжнародної науково-практичної конференції «Інформаційні технології в наукових дослідженнях і навчальному процесі», Луганськ: ЛНПУ, 2007.
16. *Бодянский Е.В., К учеренко Е.И., Михалев А.И.* Нейро-фаззи сети Петри в задачах моделирования сложных систем / Монография (научное издание). – Дніпропетровськ: Системні технології, 2005. - 311 с.
17. *Гладиш С. В.* Ймовірнісна Petri-net модель взаємодії агента безпеки з телекомунікаційною мережею // Сборник материалов XI Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», Харьков: ХНУРЭ, 2007. – с. 123.
18. ISO/IEC 15909-1 Software and Systems Engineering - High-level Petri Nets - Concepts, Definitions and Graphical Notation.
19. Питерсон Дж. Теория сетей Петри и моделирование систем. - М.: Мир, 1984. - 264 с.
20. Котов В.Е. Сети Петри. - М.: Наука, 1984. - 160 с.
21. Мурата Т. Сети Петри: Свойства, анализ, приложения // ТИИЭР. – т. 77, № 4, 1989. – с. 541-580.
22. Леоненков А. В. Нечеткое моделлирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 736 с.
23. Борисов В. В., Круглов В. В., Федулов А. С. Нечеткие модели и сети. – М.: Горячая линия – Телеком, 2007. – 248 с.

Сведения об авторах

Гладиш Сергій Вікторович, магістр телекомунікацій, аспірант, кафедра документального електрозв’язку, Одеська національна академія зв’язку ім.О.С.Попова, дом. адреса: вул..Гоголя 15а, кв.3, смт.Октябрське, Красногвардійський р-н, АР Крим, Україна, 97060, тел.+38-050-294-81-04, e-mail: sgladex@ya.ru.