УДК 338.012

МЕТОДОЛОГИЯ ПРИМЕНЕНИЯ НЕЧЕТКИХ СЕТЕЙ ПЕТРИ ДЛЯ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ РАЗРАБАТЫВАЕМОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В. И. ЗАВГОРОДНИЙ,
доктор экономических наук, профессор Департамента анализа данных, принятия решений и финансовых технологий, Финансовый университет при Правительстве России, Москва, Россия
E-mail: Vzavgorodniy@fa.ru

С. В. ФЕДОСЕЕВ,
кандидат технических наук, доцент кафедры математических методов и бизнес-информатики, Одинцовский филиал Московского государственного института международных отношений (университет) Министерства иностранных дел России, Одинцово, Россия
E-mail: fedsergvit@mail.ru

В статье представлены основные положения методологии оценки информационных рисков. Предложено использовать метод нечетких сетей Петри для оценки эффективности подсистемы управления информационными рисками разрабатываемой информационной системы. Показана работоспособность методологии на примере оценки эффективности подсистемы защиты от вредоносных программ. Предложен алгоритм предварительной проверки механизмов управления информационными рисками на совместимость, которая выполняется до начала моделирования.

Ключевые слова: нечеткие сети Петри, методология оценки информационных рисков, оценка эффективности, вредоносные программы, анализ совместимости, механизмы защиты.

Problems of management

METHODOLOGY OF USING FUZZY PETRI NETS TO ASSESS INFORMATION RISKS OF THE DEVELOPED INFORMATION SYSTEM

V. I. ZAVGORODNIY,
Doctor of Economics, Professor of Department of Data Analysis, Decision-Making and Financial Technology, Financial University under the Government of Russia, Moscow, Russia
E-mail: Vzavgorodniy@fa.ru

S. V. FEDOSEEV,
Candidate of Technique, Associated Professor of Department of Mathematical Methods and Business Informatics, Odintsovo Branch of Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of Russia, Odintsovo, Russia
E-mail: fedsergvit@mail.ru

The article presents the main provisions of the information risk assessment methodology. It is proposed to use the method of fuzzy Petri nets to assess the effectiveness of the information risk

management subsystem of the developed information system. The efficiency of the methodology is shown by the example of evaluating the effectiveness of the anti-malware subsystem. An algorithm is proposed for preliminary testing of compatibility information risk management mechanisms, which is performed prior to the start of modeling.

Keywords: *fuzzy Petri nets; information risk assessment methodology; efficiency mark; malicious programs; compatibility analysis; protection mechanisms.*

Введение. Анализ эффективности управления информационными рисками осуществляется во всех жизненных циклах информационных систем. Особую актуальность оценивание возможностей системы управления информационными рисками приобретает на этапах разработки и модернизации информационных систем. Успех решения этой проблемы во многом зависит от выбора методологии оценки информационных рисков [1].

Методология должна обеспечивать прохождение следующих этапов:

– определение объектов, целей и задач оценки информационных рисков;

– анализ особенностей объектов и условий их функционирования;

– обоснование выбора типов и классов моделей с учетом особенностей объекта;

– выбор конкретных методов и средств моделирования;

– адаптация при необходимости методов и средств к решению поставленной задачи моделирования;

– верификация моделей;

– формирование методики согласованного использования методов и средств моделирования;

– использование и развитие методики для решения практических задач.

Информационные системы относятся к классу сложных социотехнических систем. Такие системы не могут исследоваться с помощью моделей одного какого-то типа, одного метода.

Система управления информационными рисками может рассматриваться как одна из наиболее сложных подсистем информационной системы [3]. Она характеризуется наличием в основном стохастических процессов и процессов со статистической неопределенностью. Исследования процессов, в отношении которых неприменимы методы теории вероятностей и математической статистики, осуществляются с помощью методов мягких вычислений, к которым относят неточные, приближенные методы решения задач: нечеткие множества, нечеткую логику, нечеткие нейронные сети, генетические алгоритмы и эволюционное моделирование (иммунные алгоритмы, алгоритмы роевого интеллекта). Кроме того, к таким методам относят нейронные сети.

В статье приводится один из методов мягких вычислений для оценки эффективности системы предотвращения воздействия вредительских программ на ресурсы информационной системы. Данный метод основан на использовании модифицированной нечеткой сети Петри, реализующей правила нечетких продукций.

Анализ значительной части информационных рисков и оценка эффективности систем противодействия рискам связаны с использованием нечетких исходных данных. Это объясняется сложностью сбора исходных данных о негативных событиях в сфере информационной безопасности и особенностями самих событий.

Одной из причин сложности получения достоверной информации является высокая латентность инцидентов, влияющих на защищенность информационных ресурсов. Латентность инцидентов объясняется сложностью своевременного обнаружения негативного воздействия на информационные ресурсы. Кроме того, организации объективно не заинтересованы в публичности в информационной сфере инцидентов, которые могут привести к ухудшению деловой репутация организации.

Сложность обнаружения негативного инцидента, в свою очередь, обусловлена как сложностью информационных технологий, так и необходимостью дополнительных расходов на создание системы оперативного реагирования на возможные информационные риски.

Следует учитывать и преднамеренные действия злоумышленников, направленные на сокрытие или по крайней мере затруднение своевременного обнаружения негативного воздействия на информационную систему.

Негативные инциденты одного вида для конкретной организации, как правило, не носят массового характера, а сбор статистики по другим организациям затруднен не только латентностью инцидентов, но и существенными различиями информационных систем организаций и внешней информационной среды. Эти особенности не позволяют применять классические методы теории вероятностей и математи-

ческой статистики для оценки значительной доли информационных рисков.

Один из методов, позволяющих оценивать защищенность информационных систем при работе в условиях высокой неопределенности исходной информации, основан на использовании модифицированной нечеткой сети Петри, реализующей правила нечетких продукций.

Для получения показателей, характеризующих защищенность разрабатываемой, модифицируемой или эксплуатируемой информационной системы, в наибольшей степени предлагается использовать разновидность ординарной нечеткой сети Петри, которая получается в результате введения нечеткости в начальную маркировку и правила срабатывания переходов.

Нечеткое задание начальной маркировки сети позволяет моделировать степень возможности появления угроз безопасности информационным системам, а также состав и состояние режимов работы системы защиты на момент начала моделирования. Нечеткие правила срабатывания переходов могут использоваться для моделирования возможностей систем защиты противостоять информационным рискам. Дополнительная возможность моделирования правил срабатывания элементов защиты обеспечивается за счет введения пороговых значений на срабатывание переходов.

Формально модифицированная ординарная нечеткая сеть Петри может быть представлена следующим образом [2; 4]:

$$NP_f = (S, f, \lambda, m^0),$$

где $S = (P, T, I, O)$– структура нечеткой сети Петри;

I – входная функция $I: P \times T \rightarrow \{0,1\}$;

O – выходная функция $O: T \times P \rightarrow \{0,1\}$;

$f = (f_1, f_2, \dots, f_K)$ – функции принадлежности нечеткого срабатывания переходов (при $f_k \in [0,1]$);

$\lambda = (\lambda_1, \lambda_2, \dots \lambda_K)$ – значения порога срабатывания переходов (при $\lambda_k \in [0,1]$);

$$m_j^{\gamma} = \max\left\{ m_j, \quad \min\{m_n, f_k\} \right\} \quad (\forall\ p_j \in P) \wedge (O(t_k, p_j) > 0),$$
$$(n \in \{1,2,\dots,N\}) \wedge (I(p_n, t_k) > 0)$$

где f_k – значение функции принадлежности или мера возможности срабатывания перехода $t_k \in T$.

Для каждого перехода $t_k \in T$ значение функции f_k задается при формировании сети. Формула перехода к новому вектору маркировки сети используется для определения маркировки как входных, так и выходных позиций.

$m^0 = \{ m_1^0, m_2^0, \dots, m_N^0 \}$ – начальная маркировка сети, компонент которой m_n^0 является значением функции принадлежности нечеткого наличия одного маркера в n-й позиции сети, при $m_n^0 \in [0,1]$.

Рассматривается ординарная сеть Петри, в которой допускается наличие только одного маркера в позиции.

Маркировка сети меняется в соответствии с правилами.

$П_1$ – правило текущей маркировки. Состояние сети в текущий момент времени определяется вектором $m = \{ m_1, m_2, \dots, m_N \}$, компоненты $m_n \in [0,1]$ которого являются функциями принадлежности нечеткого нахождения одного маркера в позиции p_n. Исходное состояние сети определяется вектором начальной маркировки $m^0 = \{m_1^0, m_2^0, \dots, m_N^0\}$.

$П_2$ – правило активности перехода. Переход $t_k \in T$ считается активным (разрешенным), если при текущей маркировке m выполняется условие:

$$\min \{m_n\} \geq \lambda_k, \quad (n \in \{1,2,\dots,N\}) \wedge (I(p_n, t_k) > 0),$$

где λ_k – значение порога срабатывания перехода $t_k \in T$.

$П_3$ – правило нечеткого срабатывания активного перехода. Если переход $t_k \in T$ при текущей маркировке m находится в активном состоянии, то производится мгновенный переход к новому вектору маркировки $m_{\eta}^{\gamma} = \{ m_1^{\gamma}, m_2^{\gamma}, \dots, m_N^{\gamma} \}$, компоненты которого определяются в соответствии со следующим выражением:

Для рассматриваемой модификации сети Петри правила нечеткой продукции реализуются и отображаются следующим образом.

В сети правило нечеткой продукции «Правило i: Если A, то B» отображается в виде перехода $t_k \in T$ сети NP_f. В простейшем случае входной позиции p_n этого перехода соответствует условие A, а выходной позиции p_j – заключение B (рис. 1а).

Правила нечеткой продукции могут формироваться с использованием подусловий и (или) подзаключений. В этом случае возможны различные варианты формирования продукций с использованием операций нечеткой конъюнкции и нечеткой дизъюнкции, выполняемые в отношении подусловий или подзаключений.

Если условием правила нечеткой продукции определено использование нескольких подусловий и они соединены операцией нечеткой конъюнкции, то все предусловия отображаются графически в виде входных позиций соответствующего перехода (рис. 1б).

Если правилом нечеткой продукции предусмотрено использование нескольких подзаключений, которые соединены логической операцией конъюнкции, то нечеткие подзаключения отображаются в виде отдельных выходных позиций соответствующего перехода (рис.1в).

При отображении правил нечеткой продукции, в которых используются подусловия или подзаключения, объединенные логической операцией дизъюнкции, отображаются отдельный переход и позиция для каждого подусловия или подзаключения (рис. 1г, 1д).

Возможность использования нечеткой сети Петри типа NP_f для оценки эффективности систем противодействия информационным рискам проверена на примере создания модели подсистемы защиты от вредоносных программ (ПЗВП).

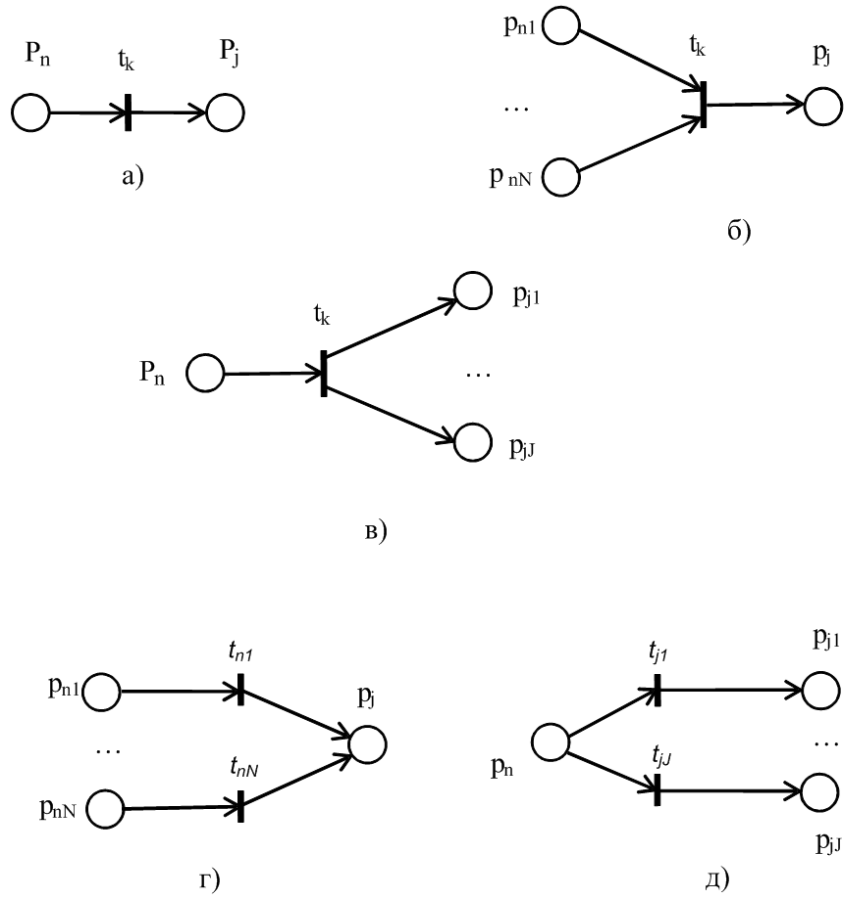

Рис. 1. Фрагменты нечетких сетей Петри для представления возможных правил нечетких продукций

Пусть требуется оценить возможности ПЗВП информационной системы (ИС). Предполагается, что противодействие вредоносной программе (ВП) осуществляется как с помощью универсальных механизмов обнаружения и блокирования ВП, так и с помощью механизмов, противодействующих конкретным типам ВП. Считается, что специализированный механизм (СМ) является более эффективным, чем универсальные механизмы.

В качестве механизма противодействия ВП могут использоваться внесение изменений в ПЗВП или общее программное обеспечение, введение в ПЗВП дополнительных программных средств, организационные мероприятия.

На первом шаге моделирования определяются правила нечетких продукций.

Правило 1. ЕСЛИ *время внедрения СМ превышает пороговое значение* ИЛИ *во внешних си-*

стемах, смежных с ИС, длительное время скрытно распространяется ВП, ИЛИ *недостаточно высока квалификация специалистов ПЗВП,* ТО *новая ВП попадет в ИС до внедрения СМ* ($f_1^1 = 0{,}45;\ f_1^2 = 0{,}4;\ f_1^3 = 0{,}2$).

Правило 2. ЕСЛИ *новая ВП попала в ИС до внедрения СМ,* И *ПЗВП не обнаружила новую ВП,* ТО *воздействие ВП на ИС не исключается* ($F_2 = 1$).

Правило 3. ЕСЛИ *новая ВП попала в ИС до начала работы СМ* И *ПЗВП способна нейтрализовать ВП без внедрения специального механизма,* ТО *воздействие ВП на ИС исключается* ($F_3 = 0{,}7$).

Правило 4. ЕСЛИ *новая ВП попала в ИС в процессе внедрения СМ,* ТО *воздействие на ИС не исключается* ($F_4 = 0{,}75$).

Правило 5. ЕСЛИ *время внедрения СМ не превышает порогового значения* И *отсутствует длительный скрытый период распространения ВП во внешних системах, смежных с ИС,* И *квалификация специалистов ПЗВП достаточно высока,* ТО *новая ВП попадает в ИС после внедрения СМ* ($F_5 = 0{,}85$).

Правило 6. ЕСЛИ *новая ВП попала в ИС после внедрения СМ,* ТО *воздействие ВП на ИС исключается* ($F_6 = 0{,}9$).

Правило 7. ЕСЛИ *сотрудники организации нарушают правила информационной безопасности,* ТО *воздействие ВП на ИС не исключается* ($F_7 = 0{,}9$).

Значения в круглых скобках означают веса или коэффициенты определенности F_i правил нечетких продукций. Эти значения в нечетких сетях Петри рассматриваются в качестве значений функций принадлежности нечеткого срабатывания переходов – f_i.

В сети каждому номеру перехода поставлено в соответствие правило нечеткой продукции с таким же номером. Исключение составляет правило под номером 1. Для отображения правила 1 используются три перехода для отображения трех высказываний, объединенных операцией нечеткой конъюнкции.

Для каждой позиции сети определены нечеткие высказывания:

– P_1 – время внедрения СМ превышает пороговое значение;

– P_2 – во внешних системах, смежных с ИС, длительное время скрытно распространяется ВП;

– P_3 – недостаточно высока квалификация специалистов ПЗВП;

– P_4 – новая ВП попадет в ИС до внедрения СМ;

– P_5 – ПЗВП не обнаружила новую ВП;

– P_6 – воздействие ВП на ИС не исключается;

– P_7 – ПЗВП способна нейтрализовать ВП без внедрения специального механизма;

– P_8 – воздействие ВП на ИС исключается;

– P_9 –новая ВП попала в ИС в процессе внедрения СМ;

– P_{10} – время внедрения СМ не превышает порогового значения;

– P_{11} – квалификация специалистов ПЗВП достаточно высока;

– P_{12} – отсутствует длительный скрытый период распространения ВП в системах, смежных с ИС;

– P_{13} – новая ВП попала в ИС после внедрения СМ;

– P_{14} – сотрудники организации нарушают правила информационной безопасности.

Зададим степень истинности некоторых высказываний V_i, которые приводятся в скобках:

– время внедрения СМ превышает пороговое значение ($V_1 = 0{,}4$);

– квалификация специалистов ПЗВП достаточно высока ($V_2 = 0{,}1$);

– во внешних системах, смежных с ИС, длительное время скрытно распространяется ВП ($V_3 = 0{,}45$);

– ПЗВП не обнаружила новую ВП ($V_5 = 0{,}8$);

– ПЗВП способна нейтрализовать ВП без внедрения специального механизма ($V_7 = 0{,}3$);

– новая ВП попала в ИС в процессе внедрения СМ ($V_9 = 0{,}1$);

– время внедрения СМ не превышает порогового значения ($V_{10} = 0{,}6$);

– отсутствует длительный скрытый период распространения ВП в системах, смежных с ИС ($V_{11} = 0{,}55$);

– квалификация специалистов ПЗВП достаточно высока ($V_{12} = 0{,}9$);

– сотрудники организации нарушают правила информационной безопасности ($V_{14} = 0{,}1$).

Приведенные значения V_1–V_{14} определяют начальную разметку нечеткой сети Петри

$$m^0 = (0{,}4;\ 0{,}1;\ 0{,}45;\ 0;\ 0{,}8;\ 0;\ 0{,}3;\ 0;\ 0{,}1;\ 0{,}6;\ 0{,}55;\ 0{,}9;\ 0;\ 0{,}1)$$

После определения начальной разметки строится модель в виде NP_f нечеткой сети Петри (рис. 2).

Процесс моделирования представляет собой пошаговый алгоритм перемещения маркеров в направлении финальных позиций P_6 и P_8.

Задача моделирования сводится к оценке возможности попадания маркера в позиции P_6 и

P_8. Для ее решения последовательно выявляются активные переходы и используются правила их нечеткого срабатывания. Если не установлены пороги срабатывания переходов, то моделирование представляется в виде выполнения определенных шагов.

Правило активизации переходов на первом шаге алгоритма выполняется для переходов t_7, t_4, t_1^1, t_1^2, t_1^3, t_5. В результате срабатывания активного перехода t_7 изменяется маркировка позиции P_6. Маркировка P_6 принимает значение $m_6 = 0{,}1$. Срабатывание активного перехода t_4 не вызывает изменения маркировки позиции P_6. Срабатывание перехода t_1^1 приведет к изменению маркировки позиции P_4 на значение $m_4 = 0{,}4$. При срабатывании активных переходов t_1^2, t_1^3 состояние маркировки позиции P_4 не изменяется ($m_4 = 0{,}4$). В результате срабатывания активного перехода t_5 состояние маркировка позиции P_{13} изменится на $m_{13} = 0{,}55$ после срабатывания перехода t_5.

Переходы t_2, t_3, t_6 становятся активными на втором шаге алгоритма. Переход t_2 срабатывает и состояние маркировки позиции P_6 изменяется с $m_6 = 0{,}1$ на маркировку $m_6 = 0{,}4$. При срабатывании перехода t_3 маркировка позиции P_8 примет значение $m_8 = 0{,}3$. Последующее срабатывание активного перехода t_6 приведет к изменению маркировки позиции P_8 на значение $m_8 = 0{,}55$.

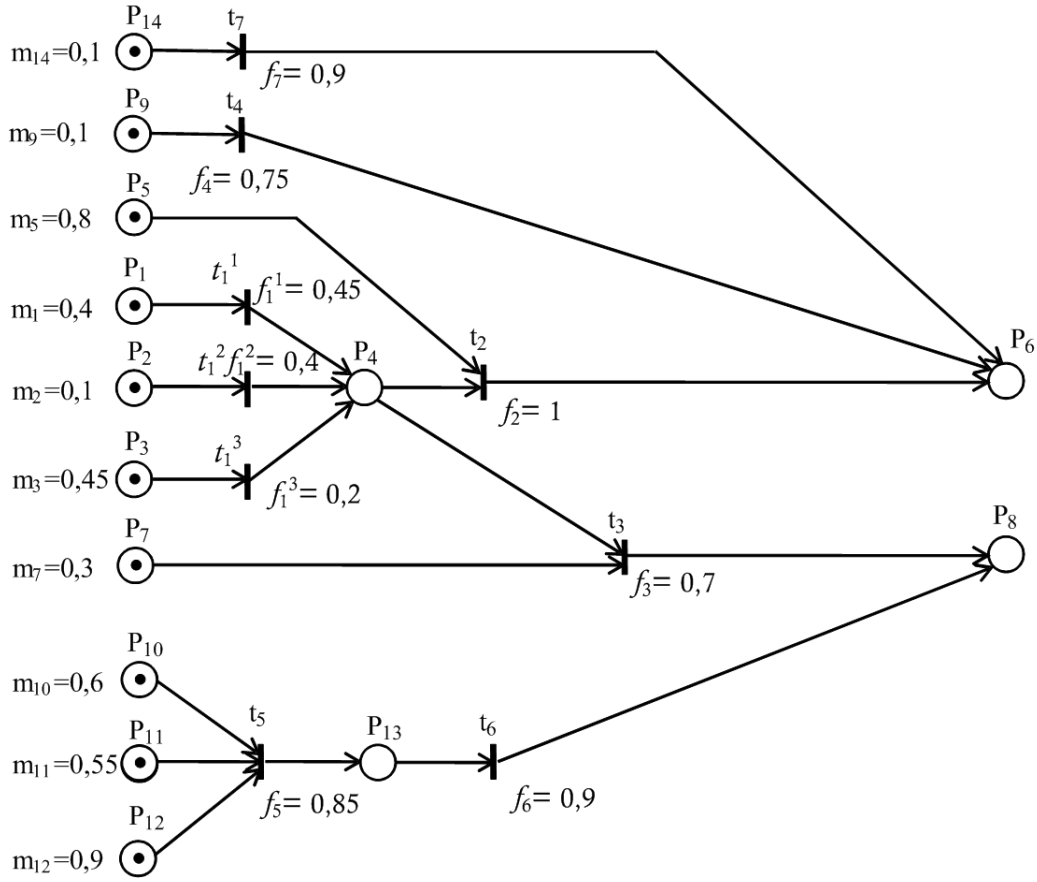

Рис. 2. Модель оценки эффективности подсистемы защиты от вредоносных программ на основе нечеткой сети Петри NP_f

Маркеры находятся только в финальных позициях P_6 и P_8. На этом работа алгоритма завершается. В позиции P_6 установлен маркер со значением $m_6 = 0{,}4$. Это означает, что степень истинности нечеткого высказывания «воздействие ВП на ИС не исключается» равна 0,4. Соответственно, степень истинности нечеткого высказывания «воздействие ВП на ИС исключается» равна 0,55, так как $m_8 = 0{,}55$.

Практическая реализация алгоритма оценки информационных рисков может выполняться с помощью программных систем MATLAB и fuzzyTECH.

Для автоматизации процесса реализации модели могут разрабатываться программы, основу которых составляли бы действия пошаговой обработки нагруженных матриц смежности, а также векторов маркировки, функций принад-

лежности нечеткого срабатывания переходов и значений порога срабатывания переходов.

При разработке новых или модификации существующих ИС необходимо оценивать множество возможных вариантов формирования архитектуры системы. Поэтому алгоритмы оценки структур должны быть дополнены новыми возможностями генерации допустимых архитектур систем.

Такие программы могут использоваться для оценки сгенерированных архитектур подсистем управления информационными рисками на итерационном шаге синтеза новых.

Алгоритм нечеткой оценки эффективности подсистем обеспечения безопасности информации может быть дополнен возможностью учета совместимости отдельных механизмов управления информационными рисками. Несовместимость механизмов может определяться аппаратной или программной несовместимостью, нецелесообразностью совместного использования механизмов вследствие дублирования функций.

Проверка на совместимость должна проводиться до моделирования процесса функционирования подсистемы защиты от информационных рисков [5]. Вариант сгенерированной структуры подсистемы проверяется на совместимость с помощью бинарной матрицы совместимости механизмов $D = \left|d_{ij}\right|, \quad d_{ij} \in [0,1], i = \overline{1,I}, j = \overline{1,J}$.

Использование проверки на совместимость позволяет решать практические задачи разработки и модификации информационных систем.

Заключение. Научное значение имеет предложенный алгоритм оценки информационных рисков, который устанавливает последовательность шагов определения значения показателей эффективности подсистемы управления информационными рисками. К научно-практическим результатам стоит отнести обоснованный выбор аппарата нечетких сетей Петри для оценивания информационных рисков разрабатываемых или модифицируемых систем. Применимость метода показана на примере оценки эффективности подсистемы защиты от вредоносных программ.

Новым научным результатом являются дополнения метода использования нечетких сетей Петри, позволяющие решать практические задачи разработки и модернизации информационных систем. Для этого предлагается выполнять предварительную проверку механизмов управления информационными рисками на совместимость до начала моделирования.

Список литературы

1. *Завгородний В. И.* Управление информационными рисками предприятия. М.: ИНИОН РАН, 2009. С. 174.
2. *Леоненков А. В.* Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург, 2005. С. 736.
3. *Федосеев С. В.* Модели расчета упущенной выгоды при заключении коммерческой сделки в условиях информационной неопределенности // Правовая информатика. 2017. № 1. С. 37–41.
4. *Штовба С. Д.* Проектирование нечетких систем средствами MATLAB. М.: Горячая линия-Телеком, 2007. С. 288.
5. *Zavgorodniy V., Lukyanov P., Nazarov S.* The Selection Algorithm of Mechanisms for Management of Information Risks / 2nd International Conference on Information Technology and Quantitative Management, ITQM 2014. Procedia Computer Science. Амстердам: Elsevier, 2014. С. 440–448.

References

1. Zavgorodniy V. I. (2009) Enterprise Information Risk Management. *Moscow, INION RAS*, pp. 174.
2. Leonenkov A. V. (2005) Fuzzy simulation in MATLAB and fuzzyTECH. *Saint-Petersburg, BHV-Petersburg*, pp. 736.
3. Fedoseyev S. V. (2017) Models of calculating lost profits in the conclusion of a commercial transaction in the conditions of information uncertainty. *Legal informatics*, no 1, pp. 37–41.
4. Shtovba S. D. (2007) Design of fuzzy systems using MATLAB. *Moscow, Hotline-Telecom*, pp. 288.
5. Zavgorodniy V., Lukyanov P., Nazarov S. (2014) The Selection Algorithm of Mechanisms for Management of Information Risks / 2nd International Conference on Information Technology and Quantitative Management, ITQM 2014. Procedia Computer Science. *Amsterdam, Elsevier*, pp. 440–448.