ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

MATHEMATICAL MODELING

Научная статья
УДК 004.056
https://doi.org/10.24143/2072-9502-2026-2-111-120
EDN LWOGAC

Модель оценки рисков информационной безопасности территориально-распределенной системы органов внутренних дел на основе нечеткой логики

Александр Анатольевич Нечай

Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, Санкт-Петербург, Россия, webexpromt@mail.ru

Аннотация. Рассматривается проблема количественной оценки рисков информационной безопасности для специфического класса систем – территориально-распределенных информационных систем органов внутренних дел. Ключевое методологическое затруднение при применении традиционных подходов в данной предметной области связано с системным дефицитом достоверной статистики об инцидентах, обусловленным как закрытым характером деятельности, так и уникальностью многих угроз. В качестве решения предлагается математическая модель, основанная на аппарате теории нечетких множеств и нечеткого логического вывода, адаптированная для работы в условиях высокой неопределенности. Модель оперирует качественными экспертными суждениями, формализованными через лингвистические переменные «Ценность актива», «Вероятность угрозы» и «Степень уязвимости». Механизм вывода реализован на основе полной базы из 27 продукционных правил и алгоритма Мамдани, результатом работы которого является количественная оценка интегрального «Уровня риска». Верификация модели проведена путем вычислительного эксперимента, имитирующего 3 характерных сценария эксплуатации систем: мобильный доступ через потенциально враждебные сети, защищенный обмен данными по выделенным каналам и внутреннюю инсайдерскую угрозу. Результаты эксперимента демонстрируют адекватную, логически непротиворечивую реакцию модели, корректно идентифицирующую критические и приемлемые состояния. Визуализация в виде поверхности отклика подтверждает нелинейный характер зависимости итогового риска от входных параметров. Практическая значимость исследования заключается в возможности интеграции разработанной модели в системы поддержки принятия решений для обоснованного планирования мер защиты и оптимального распределения ресурсов в условиях неполноты исходных данных.

Ключевые слова: информационная безопасность, оценка рисков, нечеткая логика, нечеткий вывод, лингвистическая переменная, алгоритм Мамдани, территориально-распределенная информационная система, органы внутренних дел

Для цитирования: *Нечай А. А.* Модель оценки рисков информационной безопасности территориально-распределенной системы органов внутренних дел на основе нечеткой логики // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2026. № 2. С. 111–120. https://doi.org/10.24143/2072-9502-2026-2-111-120. EDN LWOGAC.

Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2026. № 2
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)
Математическое моделирование

Original article

Fuzzy logic-based model for information security risk assessment of a territorially distributed internal affairs system

Alexander A. Nechay

Saint-Petersburg University of the Ministry of the Interior of the Russian Federation,
Saint Petersburg, Russia, webexpromt@mail.ru

Abstract. The problem of quantifying information security risks for a specific class of systems – geographically distributed information systems of law enforcement agencies is considered. The key methodological difficulty in applying traditional approaches in this subject area is associated with a systemic lack of reliable incident statistics, caused by both the confidential nature of operations and the uniqueness of many threats. As a solution, a mathematical model based on the apparatus of fuzzy set theory and fuzzy logic inference, adapted to operate under conditions of high uncertainty, is proposed. The model operates with qualitative expert judgments, formalized through the linguistic variables “Asset value”, “Threat probability”, and “Vulnerability degree”. The inference mechanism is implemented based on a complete knowledge base of twenty-seven production rules and the Mamdani algorithm, the output of which is a quantitative assessment of the integral “Risk level”. Model verification was conducted through a computational experiment simulating three characteristic system operation scenarios: mobile access through potentially hostile networks, secure data exchange via dedicated channels, and an internal insider threat. The experiment results demonstrate the model's adequate and logically consistent response, correctly identifying critical and acceptable states. Visualization in the form of a response surface confirms the nonlinear nature of the dependence of the resulting risk on the input parameters. The practical significance of the research, lies in the possibility of integrating the developed model into decision support systems for well-founded planning of protective measures and optimal resource allocation under conditions of incomplete initial data.

Keywords: information security, risk assessment, fuzzy logic, fuzzy inference, linguistic variable, Mamdani algorithm, territorially distributed information system, internal affairs bodies

For citation: Nechay A. A. Fuzzy logic-based model for information security risk assessment of a territorially distributed internal affairs system. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2026;2:111-120. (In Russ.). https://doi.org/10.24143/2072-9502-2026-2-111-120. EDN LWOGAC.

Введение

Современные процессы цифровой трансформации, активно реализуемые в России, в полной мере охватили систему Министерства внутренних дел [1]. Информационные системы органов внутренних дел (ИС ОВД), в силу самой природы решаемых ими задач, являются территориально-распределенными (ТРИС) и обладают комплексом отличительных признаков, существенно усложняющих обеспечение их безопасности [2]. К этим признакам относится иерархическая многоуровневая архитектура, предполагающая наличие протяженных и технологически неоднородных каналов связи, а также широкая номенклатура решаемых задач, требующая обработки массивов данных различной степени конфиденциальности [3]. Дополнительным усложняющим фактором выступает высокая мобильность значительной части пользовательского контингента, служебная деятельность которого связана с постоянным или эпизодическим удаленным доступом к критически важным информационным ресурсам [4]. Совокупность указанных особенностей формирует для ИС ОВД расширенную и многомерную поверхность атаки, что объективно повышает актуальность задач эффективного управления рисками информационной безопасности [5].

Традиционные методики оценки рисков, получившие широкое распространение в корпоративной среде и опирающиеся на количественные показатели вероятности реализации угрозы и размера потенциального ущерба (например, в соответствии с положениями ГОСТ Р ИСО/МЭК 27005-2010), сталкиваются со значительными методологическими трудностями при попытке их прямого применения в специфической предметной области ИС ОВД [6]. Ключевая проблема заключается в системном дефиците достоверных и репрезентативных статистических данных, необходимых для корректного расчета вероятностных метрик [7]. Данная ситуация обусловлена как закрытым характером информации об инцидентах, так и уникальностью многих атакующих воздействий на системы правоохранительных органов [8]. В этих условиях основным источником информации для анализа рисков становятся качественные экспертные оценки [9], естественным образом формулируемые на естественном языке с использованием таких категорий, как «высокая вероятность», «критическая уязвимость» или «значительный ущерб» [10]. Адекватная обработка подобных лингвистических суждений требует привлечения специального математического аппарата, спо-

собного формально работать с категориями нечеткости и неопределенности [11].

В связи с вышесказанным возникает научно-практическая задача разработки специализированной модели оценки рисков информационной безопасности [12], которая была бы свободна от жесткого требования наличия точных вероятностных входных данных и могла бы непосредственно оперировать экспертными знаниями, представленными в лингвистической форме [13]. В качестве наиболее перспективного теоретико-методологического фундамента для решения этой задачи рассматривается теория нечетких множеств Лотфи Заде и основанные на ней методы нечеткого логического вывода [14].

Научная новизна и цель исследования

Научная новизна представленной работы заключается в разработке формализованной модели комплексной оценки рисков информационной безопасности для ТРИС ОВД, которая, в отличие от классических детерминистических и вероятностных подходов, не требует точных статистических входных данных и позволяет напрямую интегрировать качественные экспертные знания [15]. Новизна определяется целенаправленной адаптацией аппарата нечеткой логики, включая теорию нечетких множеств и алгоритм нечеткого вывода Мамдани, к учету характерных для правоохранительной сферы факторов: территориальной распределенности и иерархичности архитектуры, работы с информацией ограниченного доступа, высокой мобильности пользователей и дефицита открытой статистики [16]. Предложена оригинальная структура лингвистических переменных и полная база продукционных правил, устанавливающая соответствие между комбинациями значений «Ценности актива», «Вероятности угрозы» и «Степени уязвимости» и итоговым лингвистическим «Уровнем риска». Данная модель позволяет на основе качественных экспертных суждений получать количественную оценку интегрального риска, пригодную для сравнительного анализа и поддержки принятия решений.

Целью исследования является построение, алгоритмическая реализация и экспериментальная верификация математической модели оценки рисков информационной безопасности, основанной на принципах нечеткой логики и специализированной для условий эксплуатации ТРИС ОВД.

Для последовательного достижения поставленной цели в работе решаются следующие взаимосвязанные задачи.

Первая задача заключается в формализации описания ТРИС ОВД и выделении ключевых сущностных параметров, составляющих основу для оценки риска.

Вторая задача предполагает определение состава и структуры лингвистических переменных, их терм-множеств и функций принадлежности, адекватно отражающих семантику экспертных знаний в рассматриваемой предметной области.

Третья задача состоит в разработке архитектуры системы нечеткого вывода, включающей построение полной базы нечетких продукционных правил и выбор алгоритма фаззификации, агрегации, активации и дефаззификации для получения интегральной количественной оценки.

Четвертая задача направлена на проведение вычислительного эксперимента по верификации работоспособности и адекватности модели на множестве характерных сценариев эксплуатации ИС ОВД.

Пятая задача включает анализ полученных результатов, формулировку выводов об области применимости модели и определение перспективных направлений для ее дальнейшего развития.

Модель оценки рисков информационной безопасности

Формальная основа модели начинается с представления ТРИС ОВД в виде ориентированного графа G (N, E). В данной модели множество вершин N соответствует совокупности логических и физических активов системы (серверы, рабочие станции, сегменты сети, базы данных, приложения), а множество ребер E отражает существующие между ними информационные потоки и связи. Каждый отдельный актив $a_i \in A$, где $A \subseteq N$, характеризуется атрибутом ценности для обеспечения служебной деятельности. Центральным методологическим приемом является переход от попыток получения и использования точных числовых оценок к операциям с лингвистическими переменными, что позволяет корректно включать в модель экспертные знания, выраженные на естественном языке. В качестве основы пространства оценки введены три базовые входные лингвистические переменные.

Первой и фундаментальной переменной выступает «Ценность актива» (V). Универсум переменной определен на числовой шкале от 0 до 100, а ее терм-множество включает три значения: низкая (V_L), средняя (V_M) и высокая (V_H). Функции принадлежности $\mu(x)$ для данных термов заданы параметрически с использованием Z-образной, треугольной и S-образной функций соответственно, что обеспечивает плавные переходы между качественными категориями:

$$\mu_{V_L}(x) = \begin{cases} 1, & x \le a_1, \\ 1 - 2\left(\dfrac{x - a_1}{a_2 - a_1}\right)^2, & a_1 < x \le \dfrac{a_1 + a_2}{2}, \\ 2\left(\dfrac{a_2 - x}{a_2 - a_1}\right)^2, & \dfrac{a_1 + a_2}{2} < x \le a_2, \\ 0, & x > a_2; \end{cases}$$

$$\mu_{V_M}(x) = \max\left(\min\left(\frac{x-b_1}{b_2-b_1}, \frac{b_3-x}{b_3-b_2}\right), 0\right);$$

$$\mu_{V_H}(x) = \begin{cases} 0, & x \le c_1, \\ 2\left(\frac{x-c_1}{c_2-c_1}\right)^2, & c_1 < x \le \frac{c_1+c_2}{2}, \\ 1-2\left(\frac{c_2-x}{c_2-c_1}\right)^2, & \frac{c_1+c_2}{2} < x \le c_2, \\ 1, & x > c_2, \end{cases}$$

где параметры функций a_1, a_2, b_1, b_2, b_3, c_1, c_2 определяются экспертно в процессе настройки модели. В рамках настоящего исследования были приняты следующие калибровочные значения: $a_1 = 0$, $a_2 = 40$, $b_1 = 30$, $b_2 = 50$, $b_3 = 70$, $c_1 = 60$, $c_2 = 100$.

Второй ключевой входной переменной является «Вероятность угрозы» *P*. Для удобства сопряжения модели с экспертной практикой, где оценки интуитивно даются в процентах, универсум данной лингвистической переменной также определен в диапазоне от 0 до 100, что внутри модели линейно преобразуется в математический диапазон вероятности от 0 до 1. Терм-множество переменной включает три значения: малая (P_L), умеренная (P_M), высокая (P_H). Функции принадлежности для всех термов заданы в треугольном виде с целью упрощения вычислений при сохранении достаточной выразительности:

$$\mu_{P_L}(x) = \max\left(\min\left(\frac{30-x}{30-0}, 1\right), 0\right);$$

$$\mu_{P_M}(x) = \max\left(\min\left(\frac{x-20}{50-20}, \frac{80-x}{80-50}\right), 0\right);$$

$$\mu_{P_H}(x) = \max\left(\min\left(\frac{x-60}{100-60}, 1\right), 0\right).$$

Третья входная переменная – «Степень уязвимости» *S*, отражающая наличие и серьезность известных изъянов в конфигурации или защите актива, которые могут быть использованы для реализации угрозы. Термы переменной: низкая (S_L), средняя (S_M), критическая (S_H). Функции принадлежности имеют аналогичный треугольный вид, а их конкретные параметры, определяющие положение и ширину треугольников, систематизированы в табл. 1.

Таблица 1

Table 1

Параметры функций принадлежности для лингвистической переменной «Степень уязвимости» *S*

Parameters of the membership functions for the linguistic variable "Vulnerability Degree" *S*

Терм	Тип функции	Параметр 1	Параметр 2	Параметр 3
S_L (низкая)	Треугольная	0	0	40
S_M (средняя)		20	50	80
S_H (критическая)		60	100	100

Результирующей выходной лингвистической переменной модели является «Уровень риска» *R*. Ее универсум представлен шкалой [0, 100], а термами выступают четыре качественные градации: приемлемый (R_A), повышенный (R_E), высокий (R_H), критический (R_C). Для адекватного моделирования зон переходных состояний функции принадлежности для термов *R* заданы в трапециевидной форме со следующими параметрами: R_A (0, 0, 20, 40), R_E (30, 45, 55, 70), R_H (60, 70, 80, 90), R_C (80, 90, 100, 100).

Алгоритм нечеткого вывода для расчета интегрального риска

Вычислительное ядро предложенной модели реализовано на основе алгоритма нечеткого вывода Мамдани, который хорошо зарекомендовал себя в системах, основанных на экспертных знаниях [7, 9]. Работа алгоритма осуществляется в несколько последовательных этапов, образующих цикл от четких входных данных к четкому результирующему значению.

Начальным этапом является фаззификация. На этом этапе вектор четких входных значений, полученных от эксперта или систем мониторинга для конкретной анализируемой ситуации (ценность актива v_0, вероятность угрозы p_0, степень уязвимости s_0), преобразуется в набор степеней принадлежности μ ко всем термам соответствующих лингвистических переменных. Например, для переменной *S* и четкого входного значения $S_0 = 70$ процедура фаззификации заключается в вычислении значений функций принадлежности для термов S_M и S_H в соответствии с параметрами из табл. 1, которые имеют следующий вид:

$$\mu_{S_M}(70) = \max\left(\min\left(\frac{70-20}{50-20}, \frac{80-70}{80-50}\right), 0\right) = \min(1{,}667,\ 0{,}333) = 0{,}333;$$

$$\mu_{S_H}(70) = \max\left(\min\left(\frac{70-60}{100-60}, 1\right), 0\right) = 0,250.$$

Аналогичные вычисления выполняются для переменных V и P относительно их термов.

Следующим этапом выступает агрегирование условий (антецедентов) в правилах базы знаний. Для обеспечения полноты учета всех возможных ситуаций база нечетких продукционных правил модели сконструирована как полный декартов продукт термов всех трех входных переменных, что при трех термах на каждую переменную формирует $3^3 = 27$ правил вида «ЕСЛИ (V есть V_i) И (P есть P_j) И (S есть S_k), ТО (R есть R_l)». Фрагмент базы правил представлен в табл. 2.

Таблица 2

Table 2

Фрагмент базы нечетких правил вывода

Fragment of the fuzzy inference rule base

№ п/п	Условие (ЕСЛИ)	Заключение (ТО)	№ п/п	Условие (ЕСЛИ)	Заключение (ТО)
1	V_L И P_L И S_L	R_A	15	V_M И P_H И S_M	R_H
2	V_L И P_L И S_M	R_A	16	V_M И P_H И S_H	R_C
3	V_L И P_L И S_H	R_E	17	V_H И P_L И S_L	R_A
4	V_L И P_M И S_L	R_A	18	V_H И P_L И S_M	R_E
5	V_L И P_M И S_M	R_E	19	V_H И P_L И S_H	R_H
6	V_L И P_M И S_H	R_E	20	V_H И P_M И S_L	R_E
7	V_L И P_H И S_L	R_E	21	V_H И P_M И S_M	R_H
8	V_L И P_H И S_M	R_E	22	V_H И P_M И S_H	R_C
9	V_L И P_H И S_H	R_H	23	V_H И P_H И S_L	R_H
10	V_M И P_L И S_L	R_A	24	V_H И P_H И S_M	R_C
11	V_M И P_L И S_M	R_E	25	V_H И P_H И S_L	R_H
12	V_M И P_L И S_H	R_H	26	V_H И P_H И S_M	R_C
13	V_M И P_M И S_L	R_E	27	V_H И P_H И S_H	R_C
14	V_M И P_M И S_M	R_H			

Для каждого правила с номером n вычисляется степень истинности его антецедента α_n путем применения операции минимума (логического И) к степеням принадлежности, полученным на этапе фаззификации:

$$a_n = \min\left(\mu_{V_i}(v_0), \mu_{P_i}(p_0), \mu_{S_i}(s_0)\right).$$

После определения степеней истинности всех правил производится активация их заключений (консеквентов). В модели применяется широко распространенный метод минимума (clipping), при котором выходная функция принадлежности для терма риска R_l, ассоциированного с правилом n, «срезается» на уровне вычисленной степени истинности α_n. Формально это записывается как

$$\mu^*_{R_i} = \min\left(a_n, \mu_{R_i}(r)\right),$$

где $r \in [0, 100]$.

Далее осуществляется аккумуляция всех активированных усеченных выходных функций. Выходные нечеткие множества от всех 27 правил объединяются с помощью операции максимума, формируя итоговое агрегированное нечеткое множество для выходной переменной «Уровень риска»:

$$\mu_R^{total}(r) = \max_{n=1}^{27}\left(\mu^*_{l_n}(r)\right).$$

Финальным и ключевым этапом является дефаззификация – процедура преобразования результирующего нечеткого множества $\mu_R^{total}(r)$ в конкретное, интерпретируемое числовое значение R_{crisp}, представляющее итоговую количественную оценку риска. В модели используется широко применяемый в технических приложениях метод центра тяжести (центроида), который вычисляется по формуле

$$R_{crisp} = \frac{\int_0^{100} \mu_R^{total}(r)\, r\, dr}{\int_0^{100} \mu_R^{total}(r)\, dr}.$$

На практике, при программной реализации, интеграл вычисляется дискретно с заданным шагом по универсуму. Для шага $\Delta r = 1$ формула принимает удобный для алгоритмизации вид

$$R_{crisp} \approx \frac{\sum_{k=0}^{100} \mu_R^{total}\left(k\Delta r\right)^2 \Delta r}{\sum_{k=0}^{100} \mu_R^{total}\left(k\Delta r\right)\Delta r}.$$

Результаты эксперимента и их обсуждение

Для комплексной проверки работоспособности, адекватности и практической осмысленности предложенной модели был проведен серийный вычислительный эксперимент. Он моделировал применение модели для оценки рисков в трех различных, но характерных для повседневной и оперативной деятельности ОВД сценариях, каждый из которых задавался вектором четких входных параметров (v_0, p_0, s_0).

Первый сценарий, условно названный «Мобильный доступ», моделирует ситуацию, когда выездная оперативная группа устанавливает защищенное VPN-соединение с центральной базой данных через публичную беспроводную сеть в условиях потенциально неконтролируемой обстановки. Параметры сценария: $v_0 = 90$ (высокая ценность данных), $p_0 = 85$ (высокая вероятность перехвата или вмешательства в публичной сети), s_0 = (повышенная уязвимость мобильного канала связи).

Второй сценарий, «Защищенный обмен», описывает штатную операцию передачи служебного отчета из регионального информационного центра в головное управление по выделенному защищенному каналу связи. Параметры: $v_0 = 90$ (ценность данных остается высокой), $p_0 = 20$ (низкая вероятность успешной атаки на выделенный канал), $s_0 = 30$ (низкая степень уязвимости защищенного канала).

Третий сценарий, «Внутренняя угроза», направлен на оценку риска, связанного с попыткой несанкционированного копирования конфиденциальных данных сотрудником, обладающим легитимным доступом к информационному ресурсу. Параметры: $v_0 = 90$, $p_0 = 60$ (умеренно-высокая вероятность реализации инсайдерской угрозы), $s_0 = 90$ (критическая уязвимость, связанная с избыточными правами доступа или отсутствием контроля действий внутри периметра).

Результаты моделирования для указанных сценариев, полученные после полного цикла работы алгоритма нечеткого вывода, сведены в табл. 2. Анализ результатов показывает, что модель демонстрирует логически непротиворечивое и адекватное с экспертной точки зрения поведение. Для сценария защищенного обмена, характеризующегося низкими значениями вероятности угрозы и уязвимости при высокой ценности актива, модель выдала результат $R_{crisp} = 18{,}6$, что соответствует лингвистическому терму «приемлемый риск». В то же время сценарии, связанные с работой в неконтролируемой среде (мобильный доступ) и с инсайдерской деятельностью, были корректно идентифицированы как несущие критический риск с количественными оценками 78,2 и 84,7 соответственно. Результаты представлены в табл. 3.

Таблица 3

Table 3

Результаты оценки рисков для трех характерных сценариев

Results of risk assessment for three characteristic scenarios

Сценарий	**Четкие входы v_0, p_0, s_0**	**Степени истинности ключевых правил α_n**	**R_{crisp}**	**Лингвистическая интерпретация**
Мобильный доступ	90, 85, 75	$\alpha_{24} = 0{,}167$ $\alpha_{25} = 0{,}375$ оба вывод R_C	78,2	Критический
Защищенный обмен	90, 20, 30	$\alpha_{17} = 0{,}667$ $\alpha_{18} = 0{,}333$ вывод R_A	18,6	Приемлемый
Внутренняя угроза	90, 60, 90	$\alpha_{22} = 0{,}250$ $\alpha_{25} = 0{,}500$ вывод R_C	84,7	Критический

Более высокое значение риска для инсайдерской угрозы, по сравнению с угрозой извне при мобильном доступе, также согласуется с современными взглядами на безопасность, признающими особую опасность внутренних нарушителей.

Для наглядной демонстрации нелинейного характера работы модели и взаимного влияния параметров была построена поверхность отклика. Данная поверхность, представленная на рис. 1, отображает зависимость уровня риска R от вероятности угрозы P и степени уязвимости S при фиксированном высоком значении ценности актива $V = 85$.

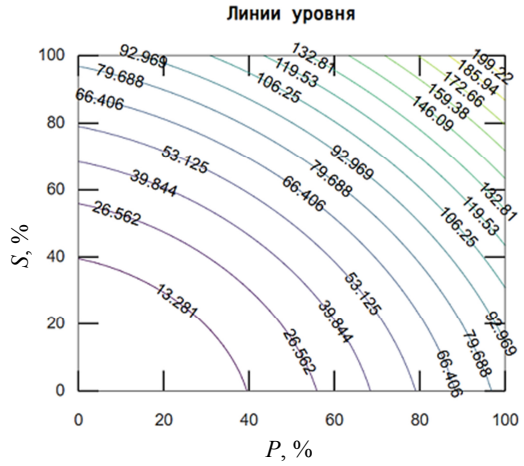

Рис. 1. Зависимость уровня риска R от вероятности угрозы P и степени уязвимости S при фиксированном высоком значении ценности актива $V = 85$

Fig. 1. Response Dependence of the risk level R on the threat probability P and the vulnerability degree S, with a fixed high asset value $V = 85$

Визуальный анализ поверхности подтверждает, что модель адекватно отражает экспертную логику: рост риска является относительно плавным при низких и средних значениях P и S, но приобретает выраженный нелинейный, почти скачкообразный характер при пересечении некоторого порога (в области $P > 50$, $S > 50$). Это соответствует зоне активации правил с выводами о высоком и критическом уровне риска и моделирует синергетический эффект, когда одновременное наличие высокой вероятности угрозы и критической уязвимости приводит к непропорционально большему увеличению интегрального риска. Такое поведение соответствует реальным условиям, когда несколько факторов уязвимости, действуя совместно, открывают возможности для реализации сложных многоэтапных атак.

Для более детального изучения характера зависимости и наглядного сопоставления с результатами вычислительного эксперимента на рис. 2 представлено семейство кривых, оно показывает зависимость уровня риска R от вероятности P при трех различных фиксированных значениях степени уязвимости S (25, 50, 75 %).

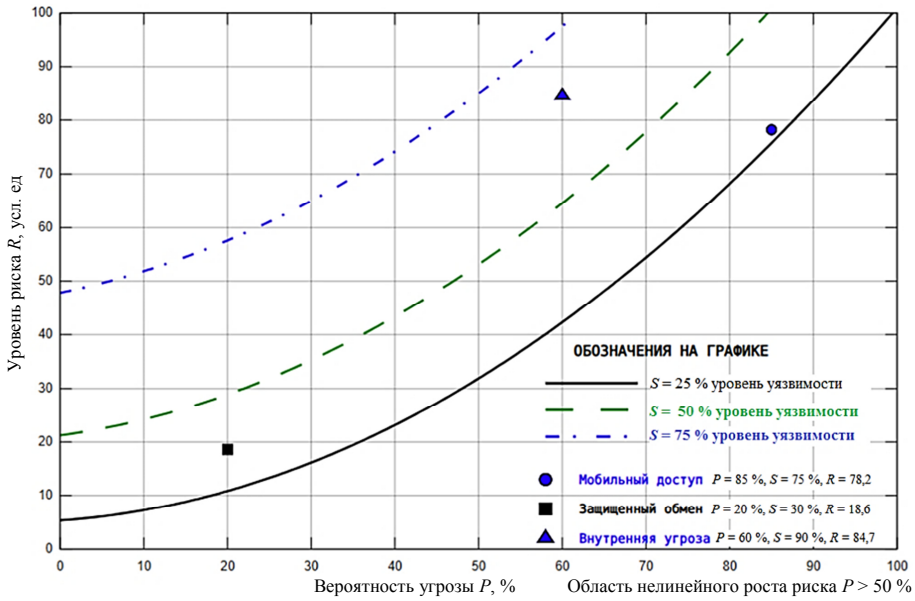

Рис. 2. Зависимость уровня риска R от вероятности угрозы P при различных фиксированных значениях степени уязвимости S (семейство кривых)

Fig. 2. Dependence of the risk level R on the threat probability P for various fixed values of the vulnerability degree S (family of curves)

Все кривые демонстрируют нелинейный рост, особенно выраженный после пересечения порога $P = 50$ %, что согласуется с поведением, наблюдаемым на трехмерной поверхности. На график нанесены точки, соответствующие трем характерным сценариям, с указанием их параметров и полученного уровня риска. Данное представление позволяет сравнить сценарии между собой и оценить вклад каждого фактора: сценарий «Защищенный обмен» попадает в зону пологого роста и приемлемого риска, в то время как сценарии «Мобильный доступ» и «Внутренняя угроза» находятся в области крутого нелинейного возрастания функции, что и обуславливает их классификацию как критические.

Предложенные графические представления являются взаимодополняющими. Трехмерная поверхность (см. рис. 1) дает целостное представление о поведении модели в области определения двух ключевых переменных, а семейство кривых (см. рис. 2) обеспечивает удобный и наглядный инструмент для точечного анализа, сравнения конкретных сценариев и демонстрации порогового эффекта, лежащего в основе нечеткой логики модели.

Заключение

В результате проведенного исследования разработана, формализована и экспериментально апробирована модель оценки рисков информационной безопасности для территориально-распределенных информационных систем органов внутренних дел. Модель построена на фундаменте теории нечетких множеств и использует алгоритм нечеткого вывода Мамдани, что составляет ее ключевое методологическое преимущество перед классическими подходами. Это преимущество заключается в принципиальной способности модели корректно обрабатывать качественные, лингвистически сформулированные экспертные оценки и проводить анализ в условиях существенной неопределенности и дефицита точных статистических входных данных, что является типичной ситуацией для рассматриваемой предметной области.

Формализация задачи оценки риска через три базовые лингвистические переменные – «Ценность актива», «Вероятность угрозы» и «Степень уязвимости» – обеспечивает достаточную для практического применения детализацию модели, сохраняя при этом ее понятность и прозрачность для экспертов-практиков в области защиты информации. Применение алгоритма нечеткого вывода с базой знаний, сформированной как полный декартов продукт термов, гарантирует учет всех возможных сочетаний входных условий, исключая пропуск потенциально опасных сценариев.

Результаты вычислительного эксперимента, включающие расчеты для трех характерных и практически значимых сценариев эксплуатации ИС ОВД, убедительно подтвердили адекватность и логическую непротиворечивость реакции модели. Модель продемонстрировала способность корректно идентифицировать критически опасные ситуации, связанные с работой в потенциально враждебной среде (мобильный доступ) и с рисками инсайдерской деятельности, и одновременно подтвердила низкий уровень риска для штатных операций, выполняемых в защищенном контуре. Визуализация в виде поверхности отклика наглядно продемонстрировала нелинейный характер зависимости итогового риска от входных параметров, адекватно моделируя синергетический эффект совместного роста угроз и уязвимостей.

Полученные результаты открывают перспективы для практического внедрения модели. Она может быть использована в качестве ядра или одного из модулей автоматизированной системы поддержки принятия решений для руководителей подразделений информационной безопасности и иных должностных лиц, ответственных за защиту информации в органах внутренних дел. На ее основе возможна разработка и формализация регламентов периодической оценки рисков, обоснованная оптимизация распределения финансовых и организационных ресурсов на закупку и внедрение средств защиты, а также планирование целевых мероприятий по повышению осведомленности и технической грамотности персонала.

В качестве перспективных направлений для дальнейшего научного поиска и развития модели рассматриваются задачи по ее структурному усложнению и повышению адаптивности. В частности, представляет интерес введение дополнительных лингвистических переменных, таких как «Квалификация нарушителя» или «Эффективность существующих контрмер», что позволит проводить более тонкую и дифференцированную оценку. Другим важным направлением является разработка и интеграция механизмов адаптивной настройки параметров функций принадлежности и весов правил на основе накопленной базы данных о реально произошедших инцидентах безопасности, что придаст модели свойства самообучения и повысит ее точность с течением времени.

Список источников

1. Смирнов Г. Г. Цифровая трансформация МВД России в разрезе проблем технического и кадрового дефицита // Мировая экономика: проблемы безопасности. 2024. № 1. С. 80–84.

2. Политкин И. А. Современные информационные системы в практике органов внутренних дел по раскрытию и расследованию преступлений // Правоохранительная функция государства: актуальные вопросы теории

и правоприменительной практики: сб. ст. науч.-представит. мероприятий (Москва, 20 ноября 2021 г.). М.: ИП Колупаева Е. В., 2022. С. 240–243.

3. Ворожбит Д. В. Автоматизированные информационные системы и банки данных органов внутренних дел // Модели и методы повышения эффективности инновационных исследований: сб. ст. по итогам Междунар. науч.-практ. конф. (Воронеж, 09 марта 2022 г.). Стерлитамак: ООО «Агентство международных исследований», 2022. С. 47–49.

4. Нечай А. А. Использование инновационных методов и современных технологий для повышения квалификации в области кибербезопасности // Азимут научных исследований: педагогика и психология. 2020. Т. 9. № 3 (32). С. 193–196. DOI 10.26140/anip-2020-0903-0043.

5. Корнилов А. А. Защита от кибератак на информационные системы органов внутренних дел // Вопросы деятельности подразделений органов внутренних дел Российской Федерации: сб. науч. тр. Тверь: Изд-во Твер. гос. ун-та, 2024. С. 107–110.

6. Лапин В. В., Слесарева Е. А., Старостенко И. Н. Информационные системы в деятельности органов внутренних дел. М.: Изд-во Моск. ун-та МВД РФ им. В. Я. Кикотя, 2014. 137 с.

7. Нечай А. А., Котиков П. Е. Методика повышения надежности функционирования систем, организованных на перепрограммируемых элементах // Вестн. Рос. нового ун-та. Сер.: Сложные системы: модели, анализ и управление. 2016. № 1-2. С. 87–89.

8. Рогожкин В. А. Защита персональных данных, обрабатываемых в информационных системах в органах внутренних дел Российской Федерации // Инновации. Наука. Образование. 2022. № 66. С. 135–143.

9. Нечай А. А., Ничагина А. В. Особенности подготовки специалистов для расследования преступлений в сфере компьютерной информации // Вестн. Санкт-Петерб. ун-та МВД России. 2025. № 4 (108). С. 251–261.

10. Yermagambetova G. T. The role of organizational agility in reducing information security risks: an economic perspective // Research forum 2024: сб. ст. IV Междунар. науч.-практ. конф. (Петрозаводск, 21 октября 2024 г.). Петрозаводск: МЦНП «Новая наука», 2024. С. 31–35.

11. Лялько А. А. Классификация нечетких систем управления // Химическая технология и техника: материалы 89-й Науч.-техн. конф. профессорско-преподават. состава, науч. сотрудников и аспирантов (с междунар. участием) (Минск, 03–18 февраля 2025 г.). Минск: Изд-во Белорус. гос. технолог. ун-та, 2025. С. 347–349.

12. Макаренко С. И., Ковальский А. А., Краснов С. А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем СПб.: Наукоемкие технологии, 2020. Т. 2. 357 с.

13. Asfha A. E., Vaish A. Information Security Risk Analysis in Food Processing Industry Using a Fuzzy Inference System // Informatics and Automation. 2023. V. 22. N. 5. P. 1083–1102. DOI 10.15622/ia.22.5.5.

14. Чернышев К. Д., Яшонков А. В. Исследование алгоритма дедуктивного нечеткого вывода в системах нечеткой логики // Старт в науке – 2024: сб. ст. IV Междунар. науч.-исследоват. конкурса (Петрозаводск, 04 ноября 2024 г.). Петрозаводск: Междунар. центр науч. партнерства «Новая Наука» (ИП Ивановская И. И.), 2024. С. 107–116.

15. Kirillova A. D., Vulfin A. M., Vasilyev V. I., Guzairov M. B. Intelligent decision support system for assessing information security risks of ICS // Modeling, Optimization and Information Technology. 2023. V. 11. N. 4 (43). DOI 10.26102/2310-6018/2023.43.4.029.

16. Нурматова Е. В., Ровинец Г. О., Сидельников А. В. Программная реализация системы нечеткого логического вывода по алгоритму Мамдани // Научная сессия НИЯУ МИФИ-2012: аннот. докл.: в 3 т. (Москва, 01–04 февраля 2012 г.). М.: Изд-во Национ. исследоват. ядер. ун-та «МИФИ», 2012. Т. 2. С. 334.

References

1. Smirnov G. G. Cifrovaya transformaciya MVD Rossii v razreze problem tekhnicheskogo i kadrovogo deficita [The digital transformation of the Ministry of Internal Affairs of Russia in the context of technical and personnel shortages]. *Mirovaya ekonomika: problemy bezopasnosti*, 2024, no. 1, pp. 80-84.

2. Politkin I. A. Sovremennye informacionnye sistemy v praktike organov vnutrennih del po raskrytiyu i rassledovaniyu prestuplenij [Modern information systems in the practice of law enforcement agencies for the detection and investigation of crimes]. *Pravoohranitel'naya funkciya gosudarstva: aktual'nye voprosy teorii i pravoprimenitel'noj praktiki: sbornik statej nauchno-predstavitel'skih meropriyatij (Moskva, 20 noyabrya 2021 g.)*. Moscow, IP Kolupaeva E. V. Publ. 2022. Pp. 240-243.

3. Vorozhbit D. V. Avtomatizirovannye informacionnye sistemy i banki dannyh organov vnutrennih del [Automated information systems and databases of law enforcement agencies]. *Modeli i metody povysheniya effektivnosti innovacionnyh issledovanij: sbornik statej po itogam Mezhdunarodnoj nauchno-prakticheskoj konferencii (Voronezh, 09 marta 2022 g.)*. Sterlitamak, OOO «Agentstvo mezhdunarodnyh issledovanij» Publ., 2022. Pp. 47-49.

4. Nechaj A. A. Ispol'zovanie innovacionnyh metodov i sovremennyh tekhnologij dlya povysheniya kvalifikacii v oblasti kiberbezopasnosti [The use of innovative methods and modern technologies to improve skills in the field of cyber security]. *Azimut nauchnyh issledovanij: pedagogika i psihologiya*, 2020, vol. 9, no. 3 (32), pp. 193-196. DOI 10.26140/anip-2020-0903-0043.

5. Kornilov A. A. Zashchita ot kiberatak na informacionnye sistemy organov vnutrennih del [Protection against cyber attacks on information systems of law enforcement agencies]. *Voprosy deyatel'nosti podrazdelenij organov vnutrennih del Rossijskoj Federacii: sbornik nauchnyh trudov*. Tver', Izd-vo Tver. gos. un-ta, 2024. Pp. 107-110.

6. Lapin V. V., Slesareva E. A., Starostenko I. N. *Informacionnye sistemy v deyatel'nosti organov vnutrennih del* [Information systems in the activities of law enforcement agencies]. Moscow, Izd-vo Mosk. un-ta MVD RF im. V. Ya. Kikotya, 2014. 137 p.

7. Nechaj A. A., Kotikov P. E. Metodika povysheniya nadezhnosti funkcionirovaniya sistem, organizovannyh na pereprogrammiruemyh elementah [A technique for improving the reliability of systems based on reprogrammable elements]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie*, 2016, no. 1-2, pp. 87-89.

8. Rogozhkin V. A. Zashchita personal'nyh dannyh, obrabatyvaemyh v informacionnyh sistemah v organah vnutrennih del Rossijskoj Federacii [Protection of personal data processed in information systems in the internal affairs bodies of the Russian Federation]. *Innovacii. Nauka. Obrazovanie*, 2022, no. 66, pp. 135-143.

9. Nechaj A. A., Nichagina A. V. Osobennosti podgotovki specialistov dlya rassledovaniya prestuplenij v sfere komp'yuternoj informacii [Features of training specialists to investigate crimes in the field of computer information]. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii*, 2025, no. 4 (108), pp. 251-261.

10. Yermagambetova G. T. The role of organizational agility in reducing information security risks: an economic perspective. *Research forum 2024: sbornik statej IV Mezhdunarodnoj nauchno-prakticheskoj konferencii (Petrozavodsk, 21 oktyabrya 2024 g.).* Petrozavodsk, MCNP «Novaya nauka » Publ., 2024. Pp. 31-35.

11. Lyal'ko A. A. Klassifikaciya nechetkih sistem upravleniya [Classification of fuzzy control systems]. *Himicheskaya tekhnologiya i tekhnika: materialy 89-j Nauchno-tekhnicheskoj konferencii professorsko-prepodavatel'skogo sostava, nauchnyh sotrudnikov i aspirantov (s mezhdunarodnym uchastiem) (Minsk, 03–18 fevralya 2025 g.).* Minsk, Izd-vo Belorus. gos. tekhnolog. un-ta, 2025. Pp. 347-349.

12. Makarenko S. I., Kovalskii A. A., Krasnov S. A. *Printsipy postroeniya i funktsionirovaniya apparatno-programmnykh sredstv telekommunikatsionnykh sistem* [Principles of construction and functioning of hardware and software of telecommunication systems]. Saint Peterburg, Naukoemkie tekhnologii Publ., 2020. Vol. 2. 357 p.

13. Asfha A. E., Vaish A. Information Security Risk Analysis in Food Processing Industry Using a Fuzzy Inference System. *Informatics and Automation*, 2023, vol. 22, no. 5, pp. 1083-1102. DOI 10.15622/ia.22.5.5.

14. Chernyshev K. D., Yashonkov A. V. Issledovanie algoritma deduktivnogo nechetkogo vyvoda v sistemah nechetkoj logiki [Investigation of the deductive fuzzy inference algorithm in fuzzy logic systems]. *Start v nauke – 2024: sbornik statej IV Mezhdunarodnogo nauchno-issledovatel'skogo konkursa (Petrozavodsk, 04 noyabrya 2024 g.).* Petrozavodsk, Mezhdunar. centr nauch. partnerstva «Novaya Nauka» (IP Ivanovskaya I. I. Publ.), 2024. Pp. 107-116.

15. Kirillova A. D., Vulfin A. M., Vasilyev V. I., Guzairov M. B. Intelligent decision support system for assessing information security risks of ICS. *Modeling, Optimization and Information Technology*, 2023, vol. 11, no. 4 (43). DOI 10.26102/2310-6018/2023.43.4.029.

16. Nurmatova E. V., Rovinec G. O., Sidel'nikov A. V. Programmnaya realizaciya sistemy nechetkogo logicheskogo vyvoda po algoritmu Mamdani [Software implementation of the Mamdani fuzzy inference system]. *Nauchnaya sessiya NIYAU MIFI-2012: annotacii dokladov: v 3 tomah (Moskva, 01–04 fevralya 2012 g.).* Moscow, Izd-vo Nacion. issledovat. yader. un-ta «MIFI», 2012. Vol. 2. P. 334.

Статья поступила в редакцию 19.01.2026; одобрена после рецензирования 09.02.2026; принята к публикации 13.04.2026
The article was submitted 19.01.2026; approved after reviewing 09.02.2026; accepted for publication 13.04.2026

Информация об авторе / Information about the author

Александр Анатольевич Нечай – кандидат педагогических наук; доцент кафедры информационной безопасности; Санкт-Петербургский университет Министерства внутренних дел Российской Федерации; webexpromt@mail.ru

Alexander A. Nechay – Candidate of Pedagogical Sciences; Assistant Professor of the Information Security Department; Saint-Petersburg University of the Ministry of the Interior of the Russian Federation; webexpromt@mail.ru