

О разработке и внедрении базовой модели информационного обеспечения принятия решений в организационных системах подразделений информационной безопасности МЧС России

В.В. Чурилина

Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург

Аннотация: В статье представлена базовая модель информационного обеспечения принятия решений, предназначенная для повышения эффективности и устойчивости организационных систем подразделений информационной безопасности МЧС России. Модель представляет собой комплексную, многоуровневую систему, основанную на взаимодействии пяти взаимосвязанных математических моделей: сбора и предварительной обработки данных, автоматической классификации, прогнозирования и анализа ситуаций, подготовки вариантов решений и управления знаниями. Для усиления функциональности и адаптивности базовой модели в неопределённых условиях введены формулы для оценки нагрузки на систему обработки данных, автоматической калибровки весовых коэффициентов на основе минимизации ошибки прогноза, расчёта индекса достоверности источников информации, взвешенной оценки событий с учётом достоверности источников, объяснимости решений на основе метода SHAP (SHapley Additive exPlanations), а также метрики полезности знаний и условий для их архивирования. Данные формулы обеспечивают объективность, прозрачность и устойчивость процессов управления, позволяя оперативно реагировать на киберугрозы, минимизировать влияние человеческого фактора и поддерживать высокое качество управленческих решений.

Ключевые слова: информационное обеспечение, принятие решений, организационная система, базовая модель, объяснимость решений, управление знаниями.

Введение.

Актуальность совершенствования процессов информационного обеспечения принятия управленческих решений в подразделениях информационной безопасности (ПИБ) МЧС России обусловлена возрастающей сложностью и динамичностью внешней неблагоприятной среды, требующей высокой оперативности, обоснованности и устойчивости управленческих воздействий. Организационные системы (ОС) ПИБ функционируют в условиях высокой информационной неопределённости [1], временных ограничений и противодействия целенаправленным угрозам, что требует применения систематизированных и научно обоснованных подходов к управлению.

В рамках решения данной задачи была разработана базовая модель [2] информационного обеспечения (БМ), призванная рационализировать и систематизировать процессы обработки информации, подготовки и выбора управленческих решений.

Основная часть.

Базовая модель информационного обеспечения принятия решений [2] предназначена для организации и рационализации процесса управления в ОС ПИБ МЧС России в условиях информационной неопределённости, временных ограничений и воздействия внешних угроз. Сущность базовой модели заключается в построении замкнутого, многоуровневого цикла информационного обеспечения, основанного на взаимодействии пяти взаимосвязанных математических моделей, каждая из которых решает определенную функциональную задачу: модель сбора и предварительной обработки данных [3], модель автоматической классификации данных, модель прогнозирования и анализа ситуаций, модель подготовки вариантов решений, модель управления знаниями.

В целях обеспечения устойчивости функционирования базовой модели в условиях высокой интенсивности киберугроз, на основе закона Литтла [4] введена метрика оценки нагрузки на систему обработки данных (1).

$$L = \frac{N_{\text{запросов}} * T_{\text{ср}}}{T_{\text{окно}}}, \quad (1)$$

где $N_{\text{запросов}}$ – количество событий, поступивших за определённый промежуток времени t ;

$T_{\text{ср}}$ – среднее время, которое требуется для обработки одного события, основанное на реальных временных метках обработки идентичных событий;

$T_{\text{окно}}$ – время, за которое считается нагрузка на систему.

Данная формула позволяет своевременно выявлять перегрузку вычислительных компонентов модели и при $L > 0,8$ инициировать механизмы приоритизации задач, что критически важно для поддержания работоспособности организационной системы ПИБ МЧС России в режиме реального времени.

Для повышения объективности и устойчивости модели [2] процесс определения весов параметров в формуле (2) переведён из экспертной оценки в режим автоматической оптимизации на основе исторических данных. Это позволяет адаптировать БМ к конкретным условиям функционирования подразделений информационной безопасности и минимизировать влияние человеческого фактора. В условиях дефицита времени и высокой ответственности такая поддержка повышает доверие к управленческим решениям. Процесс автоматической калибровки весов на основе исторических данных и оптимизации целевой функции основан на принципах минимизации средней абсолютной ошибки (MAE) [5, 6] прогноза уровня риска:

$$\min_{w_i} \sum_{t=1}^T |R_{\text{факт},t} - R_{\text{прогн},t}(w_1, w_2, \dots, w_n)|, \text{ при } \sum_{i=1}^n w_i = 1, w_i \geq 0, \quad (2)$$

где:

$R_{\text{факт},t}$ – фактический уровень риска в момент t ,

$R_{\text{прогн},t}$ – прогноз, зависящий от весов w_i ,

T – количество исторических циклов.

Калибровка проводится раз в месяц с использованием данных за предыдущие 90 дней. Средняя ошибка прогноза снизилась на 18%, стабильность модели повысилась.

Для учета достоверности различных источников (например, система обнаружения вторжений), предложено ввести индекс достоверности

источника D_s по формуле (3), который обновляется на основе точности его предыдущих сигналов. Добавление единицы в числитель и двойки в знаменатель предотвращает деление на ноль и учитывает априорное предположение о частичной достоверности нового источника.

$$D_s = \frac{N_{\text{верн}} + 1}{N_{\text{всего}} + 2} \quad (3)$$

Индекс D_s обновляется после каждого подтверждённого инцидента.

Источники с $D_s < 0,5$ исключаются из расчётов.

Формула (4) модифицирует стандартный подход к агрегированию информации, заменяя экспертные веса на динамически обновляемые индексы достоверности источников. Это повышает устойчивость модели к ложным срабатываниям и обеспечивает более точную оценку уровня угрозы, что позволяет увеличить скорость принятия управленческих решений в условиях неопределенности.

$$P(A) = \frac{\sum_{s \in S} D_s * P_s(A)}{\sum_{s \in S} D_s}, \quad (4)$$

где S – множество всех источников информации, которые сообщили о событии;

s – один конкретный источник из множества S ;

$P_s(A)$ – вероятность аномалии, оцененная источником s .

Для внедрения механизма объяснимости решений [7 – 9] предложена формула (5) на основе метода SHAP (SHapley Additive exPlanations) [10] для модели подготовки вариантов решений. В программной реализации позволяет количественно оценить вклад каждого критерия в итоговое управленческое решение, что повышает доверие ЛПР к автоматизированным рекомендациям и повышает эффективность внедрения ДИИ.

$$SHAP_i = \sum_{S \subseteq F \setminus \{i\}} \frac{|S|! * (|F| - |S| - 1)!}{|F|!} * [f(S \cup \{i\}) - f(S)], \quad (5)$$

где i – конкретный признак, вклад в общее решение которого необходимо измерить;

F – множество всех признаков, которые модель подготовки вариантов решений использует для принятия решения;

$f(S)$ – результат модели, когда используются только признаки из множества S .

Для исключения «захламления» базы знаний (далее – БЗ) устаревшими и нерелевантными записями из-за чего скорость поиска аналогичных инцидентов ИБ снизилась, влияющее на эффективность принятия решения. Для оптимизации работы модели управления знаниями [1, 2, 11] предложено создать двухуровневую систему управления знаниями, состоящую из активной БЗ (знания за последние 60 дней) и архивной БЗ (исторические данные). Для объективного ранжирования знаний в базе и поддержки её в актуальном состоянии применяется формула (6):

$$U_k = R_{эф} * e^{-\lambda \Delta t} * D_s, \quad (6)$$

где $R_{эф}$ – эффективность применения,

Δt – время с момента добавления знания в БЗ,

Автоматическое архивирование производится при условиях *if* $U_k < U_{порог}$ *или* $\Delta t > 60$ *дней then* → в архив для поддержки жизненного цикла БЗ, что позволяет использовать архивные знания только для анализа трендов в информационной безопасности.

Заключение

Совокупность исходной БМ и предложенных математических дополнений формирует мощный научно-методологический инструментарий для совершенствования управления в ПИБ МЧС России. Модель демонстрирует высокий потенциал для практического применения и может служить основой для разработки перспективных автоматизированных систем управления и поддержки принятия решений.

Литература

1. Чурилина В.В. Модели и методики совершенствования управления в организационных системах подразделений информационной безопасности МЧС России // Сибирский пожарно-спасательный вестник. 2025. № 3 (38). С. 19-33. URL: doi.org/10.34987/vestnik.sibpsa.2025.53.39.002.
2. Чурилина В. В., Билятдинов К. З. Базовая модель информационного обеспечения принятия решений в организационных системах подразделений информационной безопасности МЧС России // Современные проблемы гражданской защиты. – 2025. – № 3(56). – С. 126-135. – EDN EUQMRZ.
3. Чурилина В. В., Билятдинов К. З. Комплекс методик и модель процесса получения данных для совершенствования управления организационными системами подразделений информационной безопасности МЧС России // Инженерный вестник Дона. – 2025. – № 6. URL: ivdon.ru/ru/magazine/archive/n6y2025/10142
4. Вентцель Е. С. Исследование операций: задачи, принципы, методология. 1988. 208 с.
5. Reich N. G. et al. Case study in evaluating time series prediction models using the relative mean absolute error // The American Statistician. 2016. V. 70. №. 3. pp. 285-292.

6. Robeson S. M., Willmott C. J. Decomposition of the mean absolute error (MAE) into systematic and unsystematic components // PloS one. 2023. V. 18. №. 2. URL: pubmed.ncbi.nlm.nih.gov/36800326

7. Бирюков Д.Н., Дудкин А. С. Объяснимость и интерпретируемость — важные аспекты безопасности решений, принимаемых интеллектуальными системами (обзорная статья) // Научно-технический вестник информационных технологий, механики и оптики. 2025. №3. URL: cyberleninka.ru/article/n/obyasnimost-i-interpretiruemost-vazhnye-aspekty-bezopasnosti-resheniy-prinimaemyh-intellektualnymi-sistemami-obzornaya-statya (дата обращения: 05.09.2025).

8. Фирюлина М. А., Каширина И. Л. Описание процесса прогнозирования проблемных состояний с применением ансамблевых методов машинного обучения // Инженерный вестник Дона. 2022. №4. URL: ivdon.ru/ru/magazine/archive/n4y2022/7589.

9. Lundberg S. M., Lee S. I. A unified approach to interpreting model predictions // Advances in neural information processing systems. 2017. V. 30. URL: arxiv.org/abs/1705.07874

10. Mosca E. et al. SHAP-based explanation methods: a review for NLP interpretability // Proceedings of the 29th international conference on computational linguistics. – 2022. – P. 4593-4603.

11. Чурилина В. В. Предложения по применению комплекса методик для совершенствования управления в организационных системах // Цифровизация и технологические революции: современные вызовы и возможности: сборник статей Международной научно-практической конференции, Магнитогорск, 12 июля 2025 года. Уфа: ООО «Омега Сайнс», 2025. – С. 39-42. – EDN WXXMXED.

References

1. Churilina V. V. Sibirskiy pozharno-spatatel'niy vestnik, 2025, no. 3 (38), pp. 19–33. URL: doi.org/10.34987/vestnik.sibpsa.2025.53.39.002.
2. Churilina V. V., Bilyatdinov K. Z. Sovremennye problemy grazhdanskoй zashchity, 2025, no. 3(56), pp. 126–135. EDN EUQMRZ.
3. Churilina V. V., Bilyatdinov K. Z. Inzhenernyj vestnik Dona, 2025, № 6. URL: ivdon.ru/ru/magazine/archive/n6y2025/10142
4. Venttsel' E. S. Issledovanie operatsiy: zadachi, printsipy, metodologiya [Operations research: problems, principles, methodology]. Moskva, 1988, 208 p.
5. Reich N. G., et al. The American Statistician, 2016, vol. 70, no. 3, pp. 285–292.
6. Robeson S. M., Willmott C. J. PLOS ONE, 2023, vol. 18, no. 2. URL: pubmed.ncbi.nlm.nih.gov/36800326
7. Biryukov D. N., Dudkin A. S. Nauchno-tehnicheskij vestnik informatsionnykh tekhnologiy, mekhaniki i optiki, 2025, № 3. URL: cyberleninka.ru/article/n/obyasnimost-i-interpretiruemost-vazhnye-aspekty-bezopasnosti-resheniy-prinimaemyh-intellektualnymi-sistemami-obzornaya-statya (Accessed: 05.09.2025).
8. Firyulina M. A., Kashirina I. L. Inzhenernyj vestnik Dona, 2022, no. 4. URL: ivdon.ru/ru/magazine/archive/n4y2022/7589.
9. Lundberg S. M., Lee S. I. Advances in Neural Information Processing Systems, 2017, vol. 30. URL: arxiv.org/abs/1705.07874
10. Mosca E., et al. Proceedings of the 29th International Conference on Computational Linguistics, 2022, pp. 4593–4603.
11. Churilina V. V. Tsifrovizatsiya i tekhnologicheskie revolyutsii: sovremennye vyzovy i vozmozhnosti: sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Magnitogorsk, 12 iyulya 2025 goda. Ufa, Omega Sciences LLC, 2025, pp. 39–42. EDN WXXMED.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 17.09.2025 Дата публикации: 28.10.2025
