Инженерный вестник Дона, №9 (2025)
ivdon.ru/ru/magazine/archive/n9y2025/10354

Методика и алгоритмы решения задач управления по обеспечению надежности и эффективности организационных систем подразделений информационной безопасности МЧС России

В.В. Чурилина[1], *К.З. Билятдинов*[2]

[1] *Санкт-Петербургский университет ГПС МЧС России,*
[2] *Петербургский государственный университет путей сообщения Императора Александра I*

Аннотация: Представлена методика, включающая этапы контроля выполнения задач, сбора и анализа данных, определения критериев надёжности и эффективности, обоснованного выбора, доведения, выполнения и контроля результатов выполнения управленческих решений.

Разработан циклический алгоритм комплексной проверки соответствия критериям надёжности и эффективности системы, позволяющий оперативно реагировать на изменения, повышать устойчивость системы и адаптироваться к неблагоприятным воздействиям внешней среды.

Предлагаются усовершенствованные математические формулы для оценки состояния организационных систем, включающие расчёт коэффициента готовности, уровня выполнения плановых задач и соответствия установленным требованиям.

Применение методики направлено на повышение обоснованности принимаемых решений при снижении времени принятия решений, а также для обеспечения актуальности, полноты и достоверности информации в информационных ресурсах в интересах устойчивого развития организационных систем.

Ключевые слова: алгоритмы, время, контроль, критерии надёжности и эффективности, показатели, ресурсы, управленческие решения, цикличность.

Введение. В XXI веке развитие технологий предопределило усиление зависимости достижения цели функционирования любой сложной системы от надёжности и эффективности в заданный период времени. В связи с эти особую важность приобретает формирование и развитие научно-методологического базиса решения задач управления по обеспечению надежности и эффективности организационных систем подразделений информационной безопасности МЧС России (далее – ОС).

Анализ научных исследований [1–4] показал наличие определенного задела в исследуемой предметной области. При этом в научных работах [6–8] доказана объективная необходимость учёта специфики функционирования ОС

в условиях неопределённости и возможного недостатка ресурсов и времени на выполнение задач управления.

Таким образом, с учётом особой важности обеспечения информационной безопасности (далее – ИБ) МЧС России, и всё возрастающих требований к эффективному и надёжному функционирования ОС, вполне целесообразно сформулировать следующую постановку задачи исследования: разработать методику решения задач управления по обеспечению надежности и эффективности ОС (далее – Методика), обладающую достаточной универсальностью для применения в различных ОС для снижения времени принятия обоснованных управленческих решений при условии выполнения требований по обеспечению эффективности и надёжности. Для этого в составе Методики разработать комплекс взаимосвязанных алгоритмов и модифицировать апробированные методы, применимые для совершенствования управления ОС и в интересах учёта особой специфики функционирования различных ОС в условиях неопределённости.

Основная часть. Назначение и область применения Методики (рис. 1) в системе ИБ МЧС России: для совершенствования управления ОС при решении задач по обеспечению надёжности и эффективности ОС путём повышении обоснованности управленческих решений, снижения затрат времени на принятие управленческих решений без затрат дополнительных ресурсов, а также для формирования информационных ресурсов развития ОС (далее – ИР).

Основная терминология Методики:

Надежность организационной системы подразделения информационной безопасности (Н) – это способность сохранять устойчивое функционирование подразделения ИБ, выполняя свои функции в условиях внешних и внутренних воздействий, таких как технические сбои, ошибки сотрудников, несанкционированный доступ и все возможные неблагоприятные воздействия внешней среды.

Эффективность ОС (Э) – это степень достижения целей и задач подразделения ИБ с минимальными затратами временных, финансовых, трудовых ресурсов и максимальным качеством выполнения работ в сфере информационной безопасности.

Критерии надежности ОС ($К_н$) – это количественные или качественные показатели, характеризующие устойчивость подразделения ИБ к внешним и внутренним воздействиям, а также ее способность к восстановлению после неблагоприятных воздействий внешней среды.

Критерии эффективности ($К_э$) – это показатели, отражающие успешность выполнения задач подразделения ИБ с учетом временных, ресурсных и качественных ограничений.

Требования к надежности и эффективности определяется на основе законодательства Российской Федерации, приказов вышестоящего руководства, специфики, условий, наличия времени и ресурсов и способствуют реализации системного и комплексного подхода к решению задач управления.

Допущение: наличие в подразделениях ИБ (далее – ПИБ) квалифицированные специалистов и исправных штатных средств автоматизированной системы управления и связи.

Ограничения:

1. Методика предполагает использование существующих сил и средств и не предусматривает изменений в организационно-штатной структуре ПИБ МЧС России.

2. Внедрение Методики должно быть реализовано без дополнительных затрат времени и ресурсов, что соответствует принципу разумной достаточности, закреплённому в Концепции информационной безопасности МЧС России.

Схема алгоритма Методики (рис.1) представляет собой циклический процесс управления ОС, направленный на обеспечение высокой степени надежности и эффективности функционирования ПИБ.

Алгоритм включает этапы анализа, принятия решений, реализации и контроля, что позволяет обеспечить непрерывное совершенствование деятельности ПИБ.

Циклический характер алгоритма Методики (рис.1) позволяет оперативно реагировать на изменения, повышать надежность и эффективность работы системы, адаптироваться к новым условиям и накапливать опыт для более обоснованного принятия решений.

Начало процесса: решение ЛПР о выполнении задач управления. Процесс начинается с инициализации задачи по совершенствованию выполнения управленческих решений в рамках обеспечения надёжности и эффективности организационной системы подразделения информационной безопасности.

На этапе «Контроль выполнения текущих задач управления» осуществляется оценка степени выполнения ранее поставленных целей, соблюдения регламентов, а также соответствие деятельности установленным критериям надежности и эффективности.

Этап «Уточнение и анализ требований к надежности и эффективности» служит предназначен для формализации требований к надежности ОС ПИБ и определяет количественные и качественные параметры, которым должна соответствовать система в условиях внешних и внутренних воздействий в соответствии с установленными нормами и стандартами.

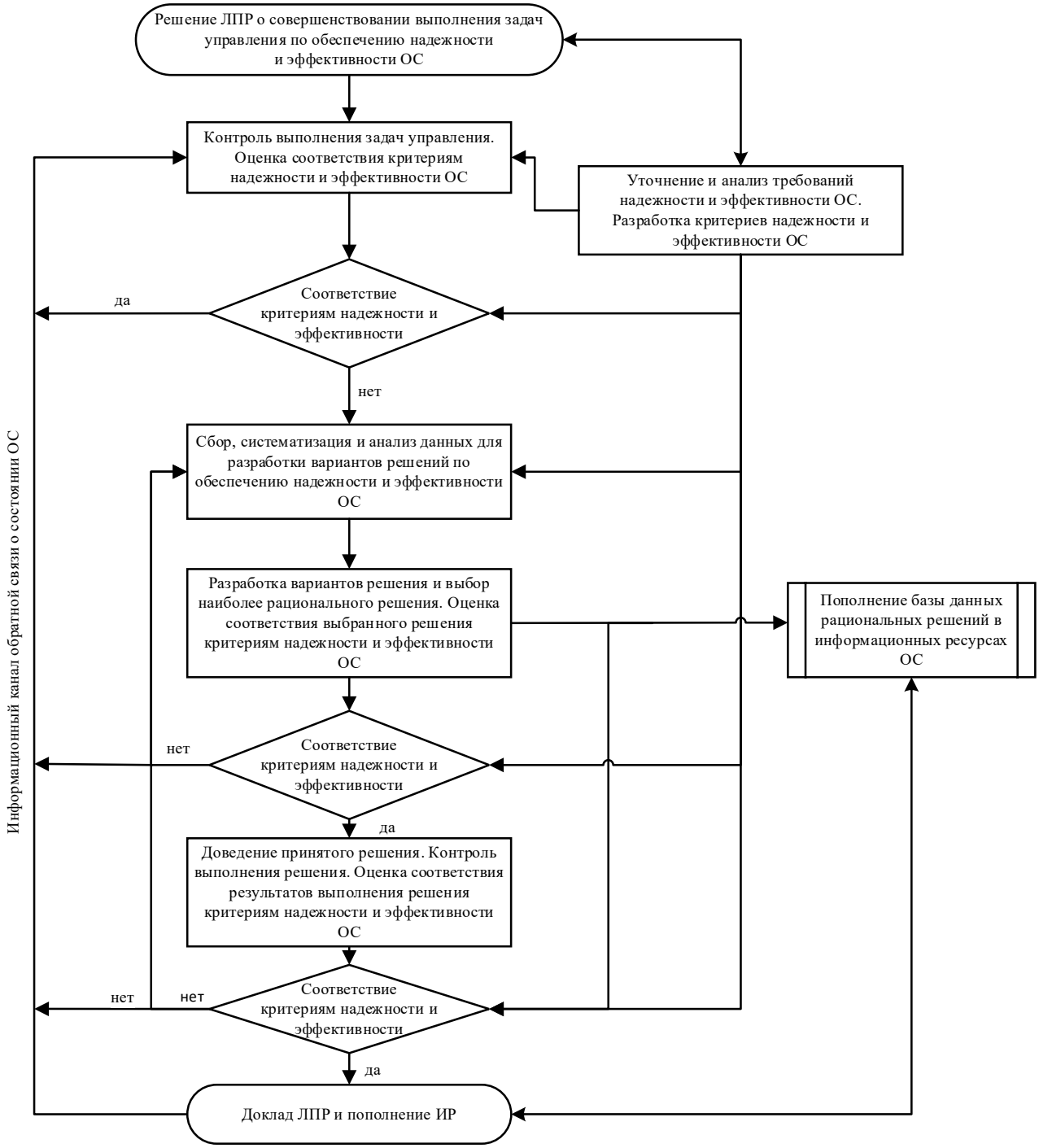

Рис. 1. – Схема алгоритма методики решения задач управления по обеспечению надежности и эффективности ОС ПИБ

Концепция ИБ МЧС России определяет допустимый уровень защищенности, обеспечивающий приемлемый уровень целостности и доступности информации [1]. В соответствии с ГОСТ Р 27.102-2021

«Надежность в технике. Надежность объекта. Термины и определения» в разработанной Методике для ОС сформированы следующие понятия и усовершенствованы расчётные формулы (1), (2), (3) и (4) в интересах выполнения задач управления:

1. Безотказность – является свойством системы непрерывно сохранять работоспособность в течение определенного времени, формула (1):

$$Б = \frac{\Sigma(T_{раб})}{n} \quad (1)$$

2. Ремонтопригодность средств связи, автоматизации и других средств, применяемых должностными лицами ПИБ (далее – ДЛ) для решения задач управления – свойство системы, заключающееся в приспособленности к предупреждению и обнаружению причин отказа, а также к восстановлению работоспособности путем обслуживания, формула (2);

$$Р = \frac{\Sigma(T_{восст})}{n} \quad (2)$$

3. Готовность – свойство системы быть в состоянии выполнять требуемую функцию в установленное время при соблюдении заданных условий эксплуатации, формула (3):

$$Г = \frac{T_{раб}}{T_{раб}+T_{вост}}, \quad (3)$$

В Методике формулы (1), (2), (3) служат основой для расчёта критерия надежности ($К_н$) для конкретной ОС, формула (4):

$$К_н = < Б, Р, Г > \quad (4)$$

где $T_{раб}$ – время функционирования ОС между простоями (сбоями) в работе;

$t_{восст}$ – время восстановления по каждому простою (сбою) системы;

n – количество зарегистрированных сбоев в работе ОС.

Расчёт критерия эффективности для конкретной ОС, формула (5):

$$К_э = < E, Y, S > \quad (5)$$

где E – это процент выполненных задач, формула (6):

$$E = \frac{Р_{факт}}{Р_{план}} * 100\% \quad (6)$$

Y – это уровень предотвращённых инцидентов ИБ, формула (7):

$$Y = \frac{И_{пр}}{И} * 100\% \quad (7)$$

S – это уровень соответствия установленным нормам и стандартам, формула (7):

$$S = \frac{\sum(Тр_{вып})}{\sum Тр} * 100\% \quad (8)$$

Соответственно, в формулах (6), (7) и (8):

$Р_{факт}$ – фактические результаты управления ОС;

$Р_{план}$ – плановые результаты управления ОС;

$И_{пр}$ – предотвращенные инциденты до причинения ущерба;

$И$ – все инциденты ИБ;

$Тр_{вып}$ – выполненные требования норм и стандартов защиты информации;

$Тр$ – все требования.

Далее на этапе проверки соответствия критериям надежности и эффективности (рис. 1) предлагается реализовать разработанный цикл процесса управления посредством проверки выполнения двух условий:

1. «Да» → Отправка данных на информационный канал обратной связи о состоянии ОС для актуализации информации о задачах управления, критериях надежности и эффективности ОС.

2. «Нет» → Переход к сбору данных для разработки корректирующих действий (рис.1).

В случае несоответствия проводится сбор и анализ данных, связанных с выявленными проблемами (например, данные об инцидентах ИБ, сбоях систем, ошибках ДЛ ОС). Полная методика сбора, структуризации и анализа данных описана в научной работе [2].

На этапе разработки вариантов решений осуществляется формирование и анализ возможных вариантов управленческих решений, направленных на повышение уровня надёжности и эффективности ОС. Этот процесс включает выработку альтернативных мер, их оценку по заранее определённым критериям, а также выбор наиболее рационального варианта.

Основными направлениями разработки решений являются:

1. Устранение выявленных отклонений на основе результатов оценки соответствия $К_н$ и $К_э$.

2. Совершенствование взаимодействия структурных подразделений ОС и других взаимодействующих с ними подразделений МЧС России.

3. Подготовка сотрудников МЧС России [3] в интересах повышения уровня $К_н$ и $К_э$.

В Методике (рис. 1) для разработки вариантов решений применяется метод рейтингового управления, присваивающий информационным системам, сотрудникам и подразделениям количественную оценку уровня риска (рис. 2).

На основе собранных данных и установленных критериев (рис.1, 2), каждому объекту присваивается числовой балл или категория (низкий, средний, высокий уровень риска) где выявляется итоговый рейтинг R по формуле (9):

$$R = w_1 * C + w_2 * V + w_3 * T, \quad (9)$$

где C – критичность информации;

V – уровень уязвимости системы;

T – частота угроз;

w_1, w_2, w_3 – весовые коэффициенты.

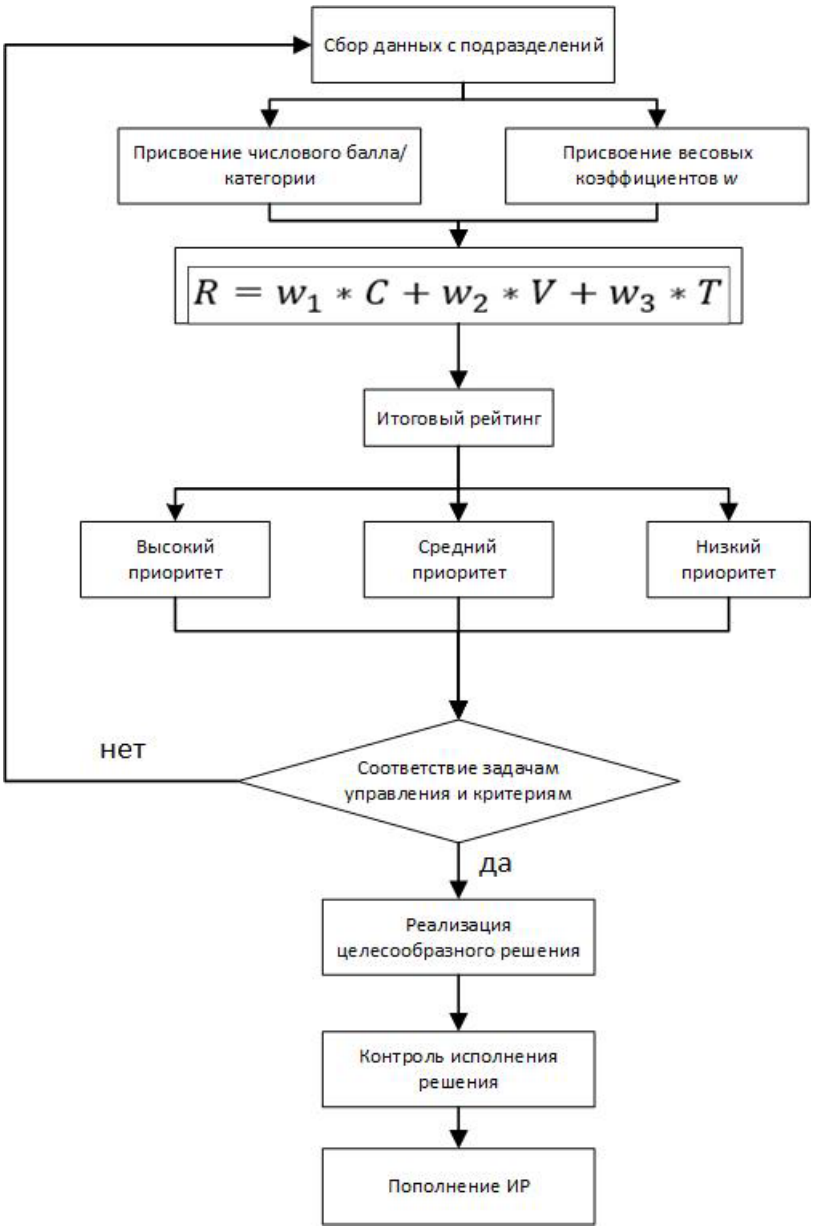

Рис. 2. – Алгоритм применения рейтингового управления

После выявления итогового рейтинга (R), объекты разбиваются на группы [5] по уровню риска (высокий приоритет из-за высокого уровня риска, средний приоритет со средним риском, низкоприоритетные объекты). На основе рейтинга принимаются решения на выполнение какой задачи уделить особое внимание для реализации задач управления.

Выбор наиболее рационального решения осуществляется путем сравнительного анализа предложенных вариантов управленческих решений, сформированных на предыдущем этапе, и принимается решение о реализации наиболее рационального решения.

Предлагаемый процесс основан на системном подходе к оценке альтернатив по заранее определённым критериям [9-11], таким как: степень соответствия нормативно-правовой базе, стоимость реализации, ожидаемый эффект, временные затраты, влияние на готовность системы к реагированию, масштабируемость и устойчивость к будущим угрозам.

После доведения принятого решения выполняются мероприятия, предусмотренные выбранным решением и контроль их исполнения на соответствие задачам управления ОС (рис.1).

Все рациональные решения пополняют базу данный рациональных решений в ИР для обеспечения информационной обеспечения управления ОС.

В Методике реализован цикл повторной проверки соответствия критериям надежности и эффективности:

1. «Да» → Переход к доведению принятого решения ЛПР с последующей оценкой соответствия результатов выполнения решения критериям надежности и эффективности ОС.

2. «Нет» → Переход к сбору данных для разработки корректирующих действий для более эффективного выполнения задач управления.

Перед докладом ЛПР предлагается провести дополнительный 3 (третий) цикл проверки соответствия критериям после выполнения принятого управленческого решения (рис.1):

1. «Да» → Завершение цикла и доклад ЛПР с последующим пополнением ИР.

2. «Нет» → Возврат к этапу сбора данных и представление данных по информационному каналу обратной связи для своевременной корректировки выполнения задач управления по обеспечению надёжности и эффективности ОС.

По окончании третьего цикла формируется отчет для ЛПР о проделанной работе, достигнутых результатах и выявленных проблемах.

ИР пополняются актуальной информацией в интересах системного и комплексного развития ОС и обеспечению ИБ МЧС России.

Заключение. Научная новизна методики заключается в разработке научно-методологических основ реализации комплексного и системного подходов к выполнению задач управления ПИБ МЧС России, основанных на циклическом алгоритме, объединяющем методы рейтингового управления и автоматизированный сбор и анализ данных.

Теоретическая значимость заключается в том, что предложенные показатели и усовершенствованные математические формулы для расчёта критериев надёжности и эффективности ОС адаптированы под специфику функционирования структурных подразделениях ПИБ МЧС России в условиях неопределенности.

Практическая значимость методики состоит в повышении обоснованности принимаемых решений при снижении времени принятия решений, а также в обеспечении актуальности, полноты и достоверности информации в ИР ОС.

В перспективе методика может выступать, как основа для внедрения в процессы управления ОС доверенного искусственного интеллекта в интересах существенного сокращения времени информационного цикла управления в условиях чрезвычайных ситуаций.

Литература

1. Беседина С. В., Жилин А. Л. Информационная безопасность в системе МЧС России // Современные технологии обеспечения гражданской обороны и

ликвидации последствий чрезвычайных ситуаций. 2011. №1 (2). URL: cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-sisteme-mchs-rossii (дата обращения: 29.05.2025).

2. 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.

3. Линник В. А., Чурилина В. В., Шестаков А. В. Комплексная методика оценки дефицита компетенций в ведомственных системах обеспечения информационной безопасности // Вестник Воронежского института ФСИН России. – 2024. – № 4. – С. 98-115.

4. Билятдинов К. З., Кривчун Е. А. Управление качеством и сравнительный анализ характеристик информационных технологий // Метрологическое обеспечение инновационных технологий: Сборник статей VI Международного форума, Санкт-Петербург, 01 марта 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2024. – С. 320. – EDN PKOKPW.

5. Разумников С.В. Нечеткая модель оценки рисков внедрения облачных технологий при формировании системы безопасности // Современные наукоемкие технологии. 2019. № 10. С. 290-295. URL: top-technologies.ru/ru/article/view?id=37739 (дата обращения: 30.05.2025).

6. Буйневич М. В. Методы искусственного интеллекта в решении задачи гармонизации нормативно-правового обеспечения пожарной и информационной безопасности для интегрированных систем защиты информации // Пожарная безопасность: современные вызовы. Проблемы и пути решения: Материалы Всероссийской научно-практической конференции,

Санкт-Петербург, 18 апреля 2024 года. – СПб. Санкт-Петербургский университет ГПС МЧС России. С. 29-33. – EDN XEVUGO.

7. Бутырский Е. Ю., Матвеев А. В. Математическое моделирование систем и процессов. СПб. Информационный издательский учебно-научный центр «Стратегия будущего», 2022. – 733 с.

8. Болдырев Д.В., Колдаев А.И., Евдокимов А.А., Кочеров Ю.Н. Совершенствование методов построения экстремальных систем управления // Инженерный вестник Дона. 2023. № 10. URL: ivdon.ru/ru/magazine/archive/n10y2023/8756.

9. Сироткин А.В., Бархатов Н.И. Модель системы автоматизированного управления информационным обслуживанием // Инженерный вестник Дона. 2013. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2013/2021.

10. Canbaloğlu G., Treur J., Roelofsma P. H. M. P. Learning of safety and security management through cyberspace: an adaptive self-modeling network model for multilevel organizational learning // Using Shared Mental Models and Organisational Learning to Support Safety and Security Through Cyberspace: A Computational Analysis Approach. – Cham: Springer Nature Switzerland, 2025. – P. 59-88.

11. Tendikov N. et al. Security Information Event Management data acquisition and analysis methods with machine learning principles // Results in Engineering. – 2024. – V. 22. – P. 102254.

References

1. Besedina S. V., ZHilin A. L. Sovremennye tekhnologii obespecheniya grazhdanskoj oborony i likvidacii posledstvij chrezvychajnyh situacij. 2011. №1 (2). URL: cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-sisteme-mchs-rossii (data assessed 29.05.2025).

2. Churilina V.V., Bilyatdinov K.Z. Inzhenernyj vestnik Dona. 2025. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2025/10142.

3. Linnik V. A., Churilina V. V., Shestakov A. V. Vestnik Voronezhskogo instituta FSIN Rossii. 2024. № 4. pp. 98-115.

4. Bilyatdinov K. Z., Krivchun E. A. Metrologicheskoe obespechenie innovacionnyh tekhnologij: Sbornik statej VI Mezhdunarodnogo foruma, Sankt-Peterburg, 01 marta 2024 goda. Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet aerokosmicheskogo priborostroeniya, 2024. P. 320. EDN PKOKPW.

5. Razumnikov S.V. Sovremennye naukoemkie tekhnologii. 2019. № 10. P. 290-295 URL: top-technologies.ru/ru/article/view?id=37739 (data assessed: 30.05.2025).

6. Bujnevich M. V. Pozharnaya bezopasnost': sovremennye vyzovy. Problemy i puti resheniya: Materialy Vserossijskoj nauchno-prakticheskoj konferencii, Sankt-Peterburg, 18 aprelya 2024. SPb.: Sankt-Peterburgskij universitet GPS MCHS Rossii. pp. 29-33. EDN XEVUGO.

7. Butyrskij E. YU., Matveev A. V. Matematicheskoe modelirovanie sistem i processov [Mathematical modeling of systems and processes]. SPb. Informacionnyj izdatel'skij uchebno-nauchnyj centr «Strategiya budushchego». 2022. 733 p.

8. Boldyrev D.V., Koldaev A.I., Evdokimov A.A., Kocherov YU.N. Inzhenernyj vestnik Dona. 2023. № 10. URL: ivdon.ru/ru/magazine/archive/n10y2023/8756.

9. Sirotkin A.V., Barhatov N.I. Inzhenernyj vestnik Dona. 2013. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2013/2021.

10. Canbaloğlu G., Treur J., Roelofsma P. H. M. P. Learning of safety and security management through cyberspace: an adaptive self-modeling network model for multilevel organizational learning. Using Shared Mental Models and Organisational Learning to Support Safety and Security Through Cyberspace: A Computational Analysis Approach. Cham: Springer Nature Switzerland, 2025. pp. 59-88.

11. Tendikov N. et al. Security Information Event Management data acquisition and analysis methods with machine learning principles. Results in Engineering. 2024. Vol. 22. P. 102254.

Дата поступления: 18.06.2025

Дата публикации: 25.08.2025