Научная статья
УДК 623.4

Методический подход к оценке и обеспечению комплексной безопасности критически важных и потенциально опасных объектов военного назначения в условиях изменений факторов угроз и ресурсных ограничений

Сергей Владимирович Ульянов, Денис Анатольевич Пузань, Евгений Викторович Лыков

Аннотация. Разработан методический подход к оценке и обеспечению комплексной безопасности критически важных и потенциально опасных объектов военного назначения в условиях изменений факторов угроз и ресурсных ограничений. Предлагаемый подход, в отличие от существующих, основан на разработанной системе показателей, критериев, принципов и методов обеспечения комплексной безопасности, учитывающих комплексное влияние факторов угроз и реализуемых решений по обеспечению безопасности критически важных и потенциально опасных объектов на эффективность функционирования критичных элементов системы комплексной безопасности в различных условиях обстановки, а также величины ущерба от различных инцидентов на защищаемых объектах. Реализация данного подхода позволяет обеспечить «равнопрочность» (сбалансированность) создаваемых систем комплексной безопасности критически важных и потенциально опасных объектов по различным видам угроз, а также устойчивость их функционирования при воздействиях дестабилизирующих факторов как по отдельности, так и при различных их сочетаниях.

Ключевые слова: критически важные объекты; потенциально опасные объекты; комплексная безопасность; показатели; критерии; угрозы; инциденты; риски; ущербы

Для цитирования: Ульянов С.В., Пузань Д.А., Лыков Е.В. Методический подход к оценке и обеспечению комплексной безопасности критически важных и потенциально опасных объектов военного назначения в условиях изменений факторов угроз и ресурсных ограничений // Вооружение и экономика. 2025. №1(71). С. 42-50.

Original article

Methodological Approach to Integrated Security Assessment and Provision of Critically Important and Potentially Dangerous Military Facilities in the Context of Threat Factors Changes and Resource Constraints

Sergei V. Ulianov, Denis A. Puzan, Evgenii V. Lykov

Abstract. A methodological approach has been developed to assess and assure the integrated security of critically important and potentially dangerous military facilities in the context of threat factors changing and resource constraints. The proposed systematic approach is based on a system of principles, methods, criteria and integrated security indicators. It takes in account various threat impacts and security support activities, and operational efficiency of critical and potentially dangerous facilities in various environmants. The implementation of this approach makes it possible to ensure the “equal strength” (balance) of the integrated security systems being created for critical and potentially dangerous facilities for various types of threats, as well as the stability of their functioning under the influence of destabilizing factors both individually and in variety of different combinations.

Keywords: critically important objects; potentially dangerous objects; integrated security; indicators; criteria; threats; incidents; risks; damage

For citation: Ulianov S.V., Puzan D.A., Lykov E.V. Methodological Approach to Integrated Security Assessment and Provision of Critically Important and Potentially Dangerous Military Facilities in the Context of Threat Factors Changes and Resource Constraints. Vooruzhenie i ekonomika = Armament and Economics. 2025;71(1): 42-50. (In Russ.).

Введение

Обеспечение комплексной безопасности на объектах Вооруженных Сил (ВС) РФ является одной из важнейших задач обеспечения национальной безопасности Российской Федерации [1]. Под комплексной безопасностью (КБ) понимается состояние всесторонней защищённости персонала, инфраструктуры, окружающей природной среды критически важных и потенциально опасных объектов (КВО и ПОО) в различных условиях обстановки, в том числе в условиях совокупного (комплексного) воздействия различных деструктивных факторов внешних и внутренних угроз, проявляющихся при создании и эксплуатации данных объектов, при котором отсутствует недопустимый риск нанесения ущерба.

© Ульянов С.В., Пузань Д.А., Лыков Е.В., 2025

Одна из возможных классификаций угроз безопасности КВО и ПОО военного назначения представлена в таблице 1 [2].

Таблица 1 – Перечень угроз безопасности КВО и ПОО

Класс угроз	Вид угроз
Военные угрозы	Угроза воздействия ядерного оружия
	Угроза воздействия химического оружия
	Угроза воздействия биологического оружия
	Угроза воздействия высокоточного оружия
	Угроза воздействия оружия на новых физических принципах
	Угроза воздействия беспилотных летательных аппаратов
	Угроза воздействия диверсионно-разведывательных групп
	Угроза воздействия обычных средств поражения
	Угроза шпионажа, разведки
Опасные природные явления	Угроза землетрясений
	Угроза наводнений (подтоплений)
	Угроза гололёда, заморозков
	Угроза снегопадов, ливней
	Угроза пожаров (лесных, степных)
	Угроза схода селей, оползней
	Угроза ураганов, гроз
	Угроза шквалов, штормов
Техногенные аварии и катастрофы	Угроза пожаров и взрывов на объектах
	Угроза аварий с невыполнением целевых задач КВО (ПОО)
	Угроза радиационных аварий
	Угроза химических аварий
	Угроза биологических аварий
	Угроза аварий на водном транспорте
	Угроза авиационных катастроф
	Угроза железнодорожных аварий
	Угроза автомобильных аварий
Антропогенные угрозы	Угроза умышленных действий
	Угроза ошибочных действий
	Угроза психических расстройств
	Угроза физиологических отклонений
	Угроза ограничений по состоянию здоровья
	Угроза низкой квалификации персонала
	Угроза низкой исполнительности персонала
	Угроза низкого уровня социальной адаптации персонала
	Угроза реализации вредных привычек
Социально-экономические угрозы *(начало)*	Угроза неразвитой инфраструктуры
	Угроза криминогенной обстановки
	Угроза эпидемий
	Угроза наркомании и алкоголизма
	Угроза гибели, травматизма (нанесения вреда здоровью)
	Угроза износа (старения) зданий, сооружений и техники

Класс угроз	Вид угроз
Социально-экономические угрозы (*окончание*)	Угроза хищения материальных средств
	Коррупционная угроза
	Угроза злоупотреблением служебным положением
Террористические угрозы	Угроза захвата, хищения ядерного оружия
	Угроза захвата заложников
	Угроза кибертерроризма
	Угроза применения взрывчатых веществ
	Угроза применения химических веществ
	Угроза применения радиационных веществ
	Угроза биотерроризма
	Угроза применения токсических веществ
	Угроза применения БПЛА в террористических целях
Угрозы безопасности информации	Угроза хищения и копирования информации
	Угроза уничтожения и модификации информации
	Угроза нарушения конфиденциальности информации
	Угроза нарушения целостности и доступности информации
	Угроза воздействия вредоносного программного обеспечения
Угрозы информационно-психологических воздействий	Угроза психологических воздействий на персонал и членов семей
	Угроза проведения незаконных публичных акций
	Угроза дискредитации лиц и государственного строя в целом
	Угроза искажения общественного мнения
Экологические бедствия	Угроза загрязнения водных объектов и почвы
	Угроза шумового загрязнения
	Угроза увеличения опасных (вредн.) отходов
	Угроза образования несанкционированных свалок отходов
Угрозы нарушений требований безопасности труда (безопасности при выполнении работ)	Угроза поражения электрическим током
	Угроза поражения при механических воздействиях
	Угроза поражения при воздействии радиоактивных веществ
	Угроза поражения при воздействии химически опасных веществ
	Угроза поражения СВЧ-излучением
	Угроза поражения при шумовом воздействии
	Угроза воздействия низких и высоких температур

Анализ существующих методов оценки и технологий обеспечения безопасности показал, что они не в полной мере отвечают современным требованиям в части комплексного учёта всех видов угроз, оперативности сбора и обработки информации, вероятности выявления угроз, достоверности оценки и контроля показателей безопасности КВО и ПОО. Задачи оценки и обеспечения безопасности КВО и ПОО по различным видам угроз в настоящее время, как правило, решаются независимо друг от друга и без учёта их возможного комплексного воздействия [1].

Кроме того, при оценке и обеспечении безопасности КВО и ПОО недостаточное внимание уделяется возможным изменениям состава и характеристик воздействующих факторов (угроз) на различных этапах жизнедеятельности защищаемых объектов. Применение новых информационных технологий, разнообразных средств разведки, беспилотных летательных аппаратов, высокоточных средств поражения большой дальности, технологий искусственного интеллекта обеспечивают высокую динамику факторов угроз и широкий спектр комплексных воздействий, способных перегрузить и снизить возможности различных защитных звеньев и системы безопасности в целом. В этой связи к перспективным системам КБ предъявляются более высокие требования по вероятности обнаружения угроз, оперативности реагированиям (быстродействию), технической готовности, устойчивости функционирования, производительности, что, в свою очередь, требует увеличения затрат ресурсов. Однако, в настоящее время отсутствуют методы обоснования требований к системам КБ, сбалансированных по различным видам угроз и ущербов от возможных инцидентов, методы оценки показателей КБ на различных этапах жизненного цикла и методы обеспечения устойчивости функционирования систем КБ КВО и ПОО военного назначения в условиях изменений факторов угроз и ресурсных ограничений. Разработке методического подхода к решению указанных задач и посвящена данная статья.

1 Принципы обеспечения комплексной безопасности критически важных и потенциально опасных объектов военного назначения в условиях изменений факторов опасности и ресурсных ограничений

Обеспечение КБ КВО и ПОО военного назначения основано на реализации комплекса конструктивно-технических решений и организационно-технических мероприятий на всех этапах их жизненного цикла, создании и применении систем, сил и средств, эффективно и устойчиво функционирующих в различных условиях обстановки и обеспечивающих требуемые уровни защищённости данных объектов от всех видов внешних и внутренних угроз при выполнении их задач.

Реализуемые решения по обеспечению КБ КВО и ПОО направлены на решение следующих основных задач:

- снижение до минимально возможных значений вероятностей реализации угроз безопасности, способных привести к инцидентам на КВО и ПОО военного назначения;
- предотвращение нештатных и чрезвычайных ситуаций при реализации угроз на КВО и ПОО;
- снижение уровней опасных воздействий на КВО и ПОО;
- обеспечение стойкости КВО и ПОО к опасным воздействиям и устойчивости системы КБ в целом;
- минимизацию ущерба от инцидентов на КВО и ПОО за счёт снижения уровней поражающих воздействий на личный состав, население и объекты окружающей среды.

На основе анализа проблемы обеспечения КБ КВО и ПОО военного назначения в условиях изменений факторов опасности и ресурсных ограничений сформулированы следующие общие принципы, реализация которых необходима для её успешного решения:

1) принцип сбалансированного задания требований к уровням защищённости (показателям КБ) КВО и ПОО от различных видов угроз с учётом ожидаемых величин ущерба (последствий) от возможных инцидентов;

2) принцип минимизации интегрального ущерба от всех видов инцидентов, возможных при создании и эксплуатации КВО и ПОО, при выполнении требований к тактико-техническим характеристикам объектов и заданных ресурсных ограничениях;

3) принцип обеспечения эффективности и устойчивости функционирования систем КБ КВО и ПОО при воздействии факторов угроз как по отдельности, так и в возможных комбинациях, в том числе при осуществлении спланированных комплексных физических, информационно-технических и информационно-психологических воздействиях, направленных на уязвимые элементы КВО и ПОО и систем их безопасности;

4) принцип верификации моделей, алгоритмов, методик и инструкций, используемых при оценке и обеспечении КБ, реагировании, локализации и ликвидации последствий инцидентов на КВО и ПОО, проверки правильности решений по обеспечению КБ в ходе испытаний и расчётно-экспериментальных работ (компьютерного моделирования);

5) принцип непрерывного мониторинга обстановки и контроля состояния КВО, ПОО и элементов систем КБ, оперативности выявления и прогнозирования угроз;

6) принцип поддержания заданных уровней готовности и эффективности функционирования элементов систем КБ КВО и ПОО, реализации превентивных мер по предотвращению и нейтрализации факторов угроз;

7) принцип систематической отработки действий должностных лиц и персонала по обеспечению КБ, парированию внешних и внутренних угроз в ходе учений и тренировок, в том числе с применением разрабатываемых учебно-тренировочных средств и программно-моделирующих комплексов.

2 Показатели и критерии эффективности решений по обеспечению комплексной безопасности критически важных и потенциально опасных объектов

Для оценки и выбора рациональных вариантов решений по обеспечению КБ КВО и ПОО разработана система показателей и критериев, представленная в таблице 2.

Таблица 2 – Система показателей и критериев эффективности решений по обеспечению КБ КВО и ПОО

Показатели КБ	
Обобщённый показатель КБ	Числовая характеристика (математическое ожидание или квантиль) случайной величины интегрального ущерба от всех видов инцидентов, возможных при создании и эксплуатации КВО и ПОО
Основные показатели КБ	Вероятности возникновения различных видов инцидентов при создании или эксплуатации КВО и ПОО в течение года
	Числовые характеристики (математические ожидания или квантили) совокупных ущербов от различных видов инцидентов, возможных при создании и эксплуатации КВО и ПОО
	Индивидуальные и коллективные риски гибели населения при создании и эксплуатации КВО и ПОО в течение года
Частные показатели КБ	Вероятности возникновения нештатных, аварийных, чрезвычайных ситуаций и их возможных исходов на различных этапах и интервалах времени создания и эксплуатации КВО и ПОО
	Числовые характеристики (математические ожидания или квантили) совокупных ущербов и их составляющих (социального, экономического, экологического и функционального ущербов) от инцидентов, возможных на разных этапах и интервалах времени создания и эксплуатации КВО и ПОО
	Риски (индивидуальные и коллективные) гибели персонала и населения при различных инцидентах, возможных на разных этапах и интервалах времени создания и эксплуатации КВО и ПОО
	Показатели достоверности контроля, оперативности, готовности, стойкости, производительности элементов системы КБ в штатных условиях и при воздействии факторов угроз (как по отдельности и в возможных их комбинациях)
Критерии эффективности решений по обеспечению КБ	
Общий критерий эффективности решений	Минимальное значение интегрального ущерба от всех видов инцидентов, возможных при создании и эксплуатации КВО и ПОО
Частные критерии эффективности (ограничения)	Непревышение заданных нормативных значений вероятностей возникновения инцидентов различной степени тяжести последствий
	Непревышение заданных нормативных значений индивидуальных и коллективных рисков для персонала и населения
	Непревышение предельных затрат и сроков разработки систем КБ КВО и ПОО и их элементов
	Выполнение требований нормативных документов и ТТЗ (ТЗ) на создание и эксплуатацию КВО и ПОО и их элементов, технических и организационных ограничений при создании и функционировании систем КБ и их элементов

3 Постановка задачи выбора рациональных вариантов решений по обеспечению комплексной безопасности критически важных и потенциально опасных объектов военного назначения в условиях изменения факторов угроз и ресурсных ограничений

Задача выбора рациональных вариантов решений по обеспечению КБ КВО и ПОО военного назначения в условиях изменения факторов угроз и ресурсных ограничений формулируется следующим образом.

Дано:

- состав и характеристики КВО и ПОО и процессов их создания и эксплуатации, $\vec{x}_{пр}(t)$;
- множество инцидентов J, возможных на различных этапах создания и эксплуатации КВО и ПОО;
- состав и характеристики факторов угроз, проявляющихся в реальных условиях создания и эксплуатации КВО и ПОО, $\vec{\varphi}(t)$;
- возможные варианты решений по обеспечению КБ КВО и ПОО на всех стадиях жизненного цикла, $\vec{\omega}(t) \in \Omega$.

Требуется:

Выбрать рациональный вариант решений по обеспечению КБ КВО и ПОО, обеспечивающий минимальное значение интегрального ущерба от всех видов инцидентов, возможных при их создании и эксплуатации, R_{Σ}:

$$\vec{\omega}^* = arg \min_{\vec{\omega}^* \in \Omega} R_{\Sigma}\left(\vec{x}_{\text{пр}}(t), \vec{\varphi}(t), \vec{\omega}(t)\right), \tag{1}$$

при ограничениях:

$$\begin{gathered} P_k\left(\vec{x}_{\text{пр}}(t), \vec{\varphi}(t), \vec{\omega}^*(t)\right) \le P_k^{\text{тр}}, k = 1, \dots, K, \\ y_s\left(\vec{x}_{\text{пр}}(t), \vec{\omega}^*(t)\right) \le (-1)^m y_s^{\text{тр}}, s = 1, \dots, S, \\ C_i\left(\vec{x}_{\text{пр}}(t), \vec{\omega}^*(t)\right) \le C_i^{\text{доп}}, i = 1, \dots, I, \\ \text{T}_i\left(\vec{x}_{\text{пр}}(t), \vec{\omega}^*(t)\right) \le T_i^{\text{доп}}, i = 1, \dots, I, \end{gathered} \tag{2}$$

где: $P_k(\cdot)$ – обеспечиваемое и требуемое значения вероятности возникновения инцидента КВО и ПОО с k-й категорией (степенью) тяжести последствий (ущерба);

$y_s(\cdot), y_s^{\text{тр}}$ – обеспечиваемые и требуемые значения s-й тактико-технической характеристики (ТТХ) КВО и ПОО;

m – индикаторная переменная, принимающая значение 0 при наличии ограничения на максимальное значение s-й ТТХ и 1 – при ограничении на минимальное значение данной характеристики;

$C_i(\cdot), T_i(\cdot), C_i^{\text{доп}}, T_i^{\text{доп}}$ – прогнозируемые значения финансовых и временных затрат на обеспечение КБ и заданные ресурсные ограничения соответственно.

4 Методы оценки и обеспечения комплексной безопасности критически важных и потенциально опасных объектов военного назначения

Для решения поставленной задачи необходимо следующее методическое обеспечение:

1) модель интегрального ущерба от инцидентов, возможных на этапах жизненного цикла КВО и ПОО;

2) стохастические сетевые модели возникновения инцидентов КВО и ПОО и статистический алгоритм оценки вероятности реализации инцидентов различной категории тяжести последствий с учётом влияния факторов угроз и реализуемых мер КБ в процессах жизненного цикла КВО и ПОО;

3) модели и алгоритмы оценки величин ущерба от различных видов инцидентов на КВО и ПОО при реализации угроз;

4) модели и алгоритмы оценки ТТХ защищаемых объектов в различных условиях обстановки с учётом реализуемых мер КБ;

5) модели и алгоритмы оценки временных и стоимостных затрат на обеспечение КБ объектов на всех стадиях их жизненного цикла;

6) алгоритмы формирования и выбора рациональных вариантов решений по обеспечению КБ КВО и ПОО;

7) методы (методики) обоснования требований, оценки и контроля показателей КБ КВО и ПОО на этапах их жизненного цикла.

Для оценки интегрального ущерба от инцидентов, возможных на этапах жизненного цикла КВО и ПОО с учётом изменений факторов угроз и реализуемых мер безопасности разработана модель, представленная аналитическим выражением:

$$R_{\Sigma} = \sum_{k=1}^{K} \sum_{l=1}^{L} \sum_{j}^{J_l} U_{klj\mu} \left(1 - \prod_{\mu=1}^{M_{kl}} \left(1 - p_{klj\mu}\right)\right)^{\delta_{kl\mu} N_{kl}}, \quad (3)$$

где: $p_{klj\mu}(\cdot)$ – вероятность возникновения инцидента j-го вида ($j = 1, \dots, J$) на l-м этапе жизнедеятельности КВО и ПОО ($l = 1, \dots, L$) и k-м интервале времени ($k = 1, \dots, K$) при μ-м сочетании факторов угроз и реализуемых мер КБ;

$\delta_{kl\mu}$ – вероятность реализации μ-го сочетания (комбинации) факторов угроз и реализуемых мер безопасности на l-м этапе функционирования КВО (ПОО) на k-м интервале времени их эксплуатации;

N_{kl} – объем (количество) процессов l-го вида, реализуемых на КВО (ПОО) на k-м интервале времени;

$U_{klj\mu}(\cdot)$ – математическое ожидание ущерба при данных сочетаниях факторов и условий.

Для оценки вероятностей возникновения инцидентов на КВО и ПОО военного назначения при различных сочетаниях факторов угроз и реализуемых мер КБ предлагается метод, основанный на разработке стохастических сетевых моделей возникновения и развития опасных процессов [3].

Стохастические сетевые модели (ССМ) описывают причинно-следственные связи и возможные пути развития аварийных процессов от исходных опасных событий – до исходов (аварий комплекса).

Типовая стохастическая сетевая модель возникновения и развития опасного процесса схематически показана на рисунке 1.

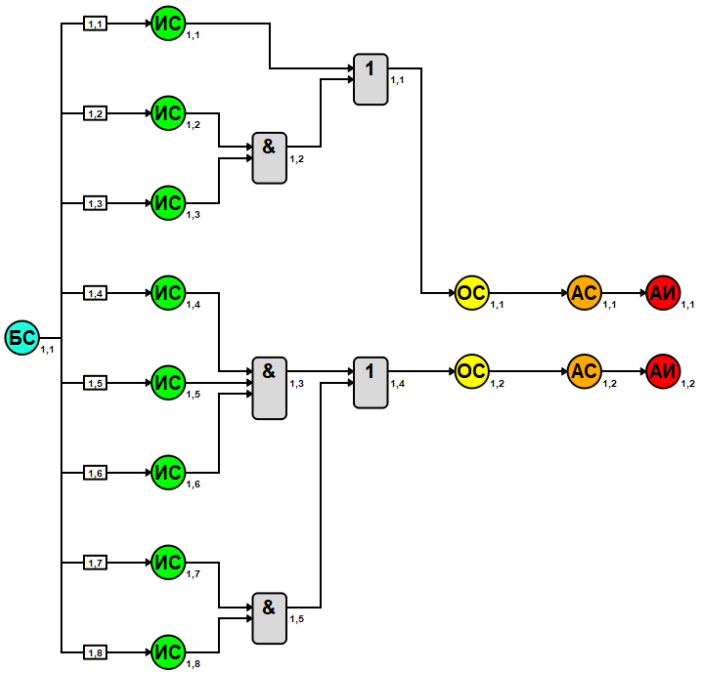

Рисунок 1 – Типовая ССМ возникновения и развития опасного процесса

На данной схеме кружками обозначены состояния развития опасного процесса, где символами обозначаются БС – безопасное состояние, ИС – исходное событие (условие предпосылка), ОС – опасное событие, АС – аварийная (чрезвычайная) ситуация, АИ – инцидент (аварийный исход) при реализации угрозы. Стрелками обозначены переходы между состояниями развития опасного процесса, прямоугольниками – барьеры безопасности. Логические операторы («И», «ИЛИ») обозначены на данной схеме символами & и 1 соответственно.

Каждый переход характеризуется условной вероятностью его преодоления, зависящей от состава воздействующих факторов и реализуемых мероприятий по обеспечению безопасности и парированию угроз.

Вероятность возникновения инцидента определяется с использованием логико-вероятностных методов, предполагающих разработку логических функций возникновения и развития случайных событий.

Для учёта данного влияния факторов угроз и реализуемых мер безопасности в качестве аппроксимирующих зависимостей предлагается использовать логистические функции вида:

$$p_\mu = \frac{1}{1+e^{-Z_\mu}}, \tag{4}$$

где Z_μ – обобщённый параметр безопасности, описываемый линейной регрессией:

$$Z_\mu = a_0\left(1 + \sum_{\mu=1}^{\text{M}} \frac{\alpha_\mu}{\alpha_0} X_\mu\right) = \alpha_0\left(1 + \sum_{\mu=1}^{\text{M}} K_\mu X_\mu\right), \tag{5}$$

a_0 – фоновое значение параметра Z_μ при отсутствии факторов угроз, определяемое с использованием выражения:

$$\alpha_0 = ln\left(\frac{p_{\text{пр}}}{1-p_{\text{пр}}}\right), \tag{6}$$

$p_{пр}$ – проектная оценка вероятности появления опасного случайного события (в отсутствии факторов повышенного риска).

X_μ – значение индикаторной функции появления μ-го сочетания факторов угроз и реализуемых мер КБ $\left(X_\mu \in [0,1]\right)$;

α_μ – весовой коэффициент μ-го сочетания факторов;

K_μ – коэффициент значимости μ-го сочетания факторов:

$$K_\mu = \frac{\alpha_\mu}{\alpha_0}. \tag{7}$$

Значения коэффициентов регрессии определяются следующим образом:

а) при наличии статистических данных по результатам испытаний и эксплуатации аналогов – с использованием стандартных статистических методов регрессионного анализа;

б) при наличии математических моделей исследуемых опасных процессов – методами математического моделирования, в том числе аналитических методов, методов теории подобия, статистического моделирования;

в) при отсутствии данных – экспертных методов оценки.

Условные вероятности переходов (преодоления «барьеров безопасности»), в свою очередь, определяются с учётом значений коэффициентов готовности, оперативности, полноты и достоверности контроля обстановки (вероятности обнаружения угроз), стойкости и производительности элементов системы КБ по формуле:

$$p_{\text{усл}_\mu} = 1 - k_{\text{Г}}^{\mu} k_{\text{Т}}^{\mu} k_{\text{ПДК}}^{\mu} k_{\text{С}}^{\mu} k_{\text{П}}^{\mu}. \tag{8}$$

Для решения задач оценки и обеспечения КБ КВО и ПОО военного назначения в постановке (1, 2) предлагается применить ряд методических приёмов, в том числе:

- проведение классификации и категорирования КВО и ПОО военного назначения;
- разработку типовых моделей угроз для различных типов КВО и ПОО;
- классификацию (категорирование) инцидентов на КВО и ПОО по степени тяжести последствий (величине потенциального ущерба). Пример одной из таких классификаций приведён в таблице 3;

- создание и применение справочников со статистическими данными для оценки вероятностей возникновения первичных (исходных) случайных событий и условных вероятностей реализации переходов в штатных условиях и при воздействии факторов угроз;
- разработку математических моделей для оценки вероятностей возникновения опасных событий на КВО и ПОО в различных условиях обстановки;
- применение шкалы вероятностей для экспертной оценки вероятностей реализации событий, которые невозможно определить с использованием других методов (таблица 4);
- разработку баз данных и электронных паспортов КБ КВО и ПОО;
- создание программно-аппаратных комплексов (автоматизированных систем) оценки, контроля и поддержки принятия решений по обеспечению КБ КВО и ПОО военного назначения;
- разработку и внедрение технологий искусственного интеллекта для оперативной обработки информации и выявления угроз безопасности КВО и ПОО по результатам мониторинга информационного пространства [4].

Таблица 3 – Четырёхуровневая классификация инцидентов на КВО и ПОО по степени тяжести последствий КВО и ПОО

Класс инцидента	Уровень тяжести последствий	Потенциальный ущерб, у.е.	Критическое значение вероятности (на один точечный объект)
A	Максимальный	$U \geq 10^6$	$P \leq 10^{-6}$
B	Высокий	$10^5 \leq U \leq 10^6$	$P \leq 10^{-5}$
C	Средний	$10^4 \leq U \leq 10^5$	$P \leq 10^{-4}$
D	Низкий	$U \leq 10^4$	$P \leq 10^{-3}$

Таблица 4 – Шкала вероятностей возникновения случайных событий при выполнении контрольных и технологических операций

Характеристика случайного события	Диапазон значений вероятности
Высоковероятные, очень частые, регулярные события	
Событие произойдёт наверняка, обязательно	$0{,}999999999 \leq P \leq 1{,}00000000$
Практически достоверное событие	$0{,}999999 \leq P < 0{,}999999999$
Событие может не произойти в исключительном случае	$0{,}99999 \leq P < 0{,}999999$
Событие может не произойти в очень редких случаях	$0{,}9999 \leq P < 0{,}99999$
Событие может не произойти в редких случаях	$0{,}999 \leq P < 0{,}9999$
Событие осуществляется с высокой вероятностью	$0{,}99 \leq P < 0{,}999$
Событие произойдёт почти несомненно	$0{,}9 \leq P < 0{,}99$
Вероятные, частые, ожидаемые события	
Очень вероятно, что событие произойдёт	$0{,}8 \leq P < 0{,}9$
Вероятно, что событие произойдёт	$0{,}7 \leq P < 0{,}8$
Событие скорее случится, чем нет	$0{,}6 \leq P < 0{,}7$
Практически равные шансы успеха и неудачи	$0{,}4 \leq P < 0{,}6$
Событие скорее не произойдёт, чем произойдёт	$0{,}3 \leq P < 0{,}4$
Сомнительно, что событие произойдёт	$0{,}2 \leq P < 0{,}3$
Событие вероятно, но вероятность его весьма низка	$0{,}1 \leq P < 0{,}2$
Маловероятные, редкие, неожиданные события	
Событие маловероятно	$0{,}01 \leq P < 0{,}1$
Событие происходит нечасто	$0{,}001 \leq P < 0{,}01$
Событие происходит редко	$0{,}0001 \leq P < 0{,}001$
Событие происходит очень редко	$0{,}00001 \leq P < 0{,}0001$
Событие может произойти в исключительном случае	$0{,}000001 \leq P < 0{,}00001$
Событие практически невозможно	$0{,}000000001 \leq P < 0{,}000001$
Событие не может произойти	$0{,}00000000000 \leq P < 0{,}000000001$

Для формирования и выбора рациональных вариантов решений по обеспечению КБ КВО и ПОО может быть использован статистический алгоритм на основе байесовской процедуры с обучением, изложенный в работе [5].

Таким образом, разработан новый методический подход к оценке и обеспечению КБ КВО и ПОО военного назначения в условиях изменений факторов угроз и ресурсных ограничений. Реализация данного подхода позволяет обеспечить сбалансированность систем КБ по различным видам угроз и устойчивость их функционирования при воздействиях дестабилизирующих факторов как по отдельности, так и при различных их сочетаниях.

Список источников

1. Колесников И.А., Коршак А.В. Система комплексной безопасности особо важных объектов Вооруженных Сил Российской Федерации как новый уровень обеспечения национальной безопасности России // Военная мысль. 2020. №2. С. 59-69.
2. Кузьмин Е.О., Кузьмина И.В. Классификация угроз национальной безопасности: правовой аспект // Вестник Национального Института Бизнеса. 2022. №2(46). С. 116-123.
3. Голенко-Гинзбург Д.И. Стохастические сетевые модели планирования и управления разработками: монография. Воронеж: Научная книга, 2010. 283 с.
4. Косаренко Н.Н. Система искусственного интеллекта: понятие, теория, право и перспективы развития : монография. М.: Ruscience, 2022. 174 с.
5. Ульянов С.В., Пузань Д.А. Методика выбора рациональных вариантов решений по обеспечению безопасности эксплуатации мобильных ракетных комплексов в условиях воздействия факторов повышенного риска // Двойные технологии. 2021. №4(97). С. 8-13.

Информация об авторах

С.В. Ульянов – доктор технических наук, старший научный сотрудник.
Д.А. Пузань – кандидат технических наук.
Е.В. Лыков – https://orcid.org/0009-0003-2856-2822.