

УДК 338

**РИСК-МЕНЕДЖМЕНТ И УСТОЙЧИВОСТЬ ОРГАНИЗАЦИИ:
ПРАКТИКА ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ****Терелецкова Е.В.***к.с.н., доцент**Уфимский университет науки и технологий**г. Уфа Российская Федерация***Ардаширова А.А.,***магистрант**Уфимский университет науки и технологий**г. Уфа Российская Федерация*

Аннотация. В статье рассматривается применение риск-менеджмента как инструмента обеспечения устойчивости организации на примере подразделений вневедомственной охраны. Предложена практико-ориентированная методология оценки рисков и устойчивости с использованием количественных метрик (среднее время реагирования, доля ложных срабатываний, коэффициент готовности) и сценарного моделирования. На основе анализа документов, статистики инцидентов и экспертных интервью выявлены ключевые риски и предложены меры по повышению устойчивости системы реагирования. Практическая значимость исследования состоит в возможности внедрения предложенных мер в деятельность охранных структур без существенных организационных затрат.

Ключевые слова: риск-менеджмент, устойчивость организации, вневедомственная охрана, матрица рисков, сценарное моделирование, метрики эффективности, управление операционными рисками.

**RISK MANAGEMENT AND ORGANIZATIONAL RESILIENCE: THE
CASE OF EXTRADEPARTMENTAL SECURITY SERVICE****Tereletskova E.V.***PhD (Social Sciences), Associate Professor**Ufa University of Science and Technology**Ufa, Russian Federation***Ardashirova A.A.,***Master's Student**Ufa University of Science and Technology**Ufa, Russian Federation*

Abstract. The paper examines risk management as a tool for ensuring organizational resilience, using the example of extradepartmental security service units. A practice-oriented methodology is proposed that combines quantitative metrics (average response time, false alarm rate, readiness coefficient) with

scenario modeling. Based on document analysis, incident statistics, and expert interviews, key risks are identified and measures to improve the resilience of the response system are proposed. The practical relevance lies in the feasibility of implementing the proposed measures in security organizations with minimal organizational costs.

Keywords: risk management, organizational resilience, extradepartmental security, risk matrix, scenario modeling, performance metrics, operational risk management.

Современные условия функционирования организаций характеризуются высокой неопределённостью и ростом числа внешних и внутренних угроз. В этих условиях устойчивость (resilience) становится не менее важным показателем эффективности, чем традиционные финансовые метрики [3, 8]. Для государственных охранных структур, к которым относится вневедомственная охрана, устойчивость особенно критична: любая задержка или ошибка может привести к материальному ущербу, репутационным потерям и даже угрозе жизни [1, 2].

Специфика вневедомственной охраны - режимность, жёсткая регламентация, высокая цена ошибки и необходимость круглосуточной готовности делает классические подходы к риск-менеджменту недостаточными без адаптации под оперативную работу [1, 6].

Цель статьи показать, как инструменты риск-менеджмента (матрица рисков, количественные метрики, сценарное моделирование) могут быть применены на практике для повышения устойчивости подразделения вневедомственной охраны.

Задачи исследования:

- идентифицировать основные риски в деятельности вневедомственной охраны;
- оценить их с помощью количественных и качественных методов;
- проанализировать устойчивость системы реагирования через метрики и сценарии;
- предложить практические меры по снижению рисков и повышению устойчивости.

Объект исследования - подразделение вневедомственной охраны, предмет - система управления рисками и её влияние на устойчивость функционирования.

В основу исследования положен системный подход к управлению рисками, закреплённый в стандартах ISO 31000:2018 и его российской адаптации ГОСТ Р ИСО 31000-2019 [1, 2]. Согласно этим документам, риск-менеджмент должен быть интегрирован в процессы управления, а не существовать как отдельный блок отчётности.

Для оценки устойчивости использована концепция организационной устойчивости (resilience), которая трактует устойчивость как способность сохранять работоспособность при сбоях и быстро восстанавливаться после

инцидентов [3, 8]. В отличие от традиционного подхода «предотвратить любой ценой», resilience-подход допускает возникновение инцидентов, но требует, чтобы система могла с ними справляться без потери ключевых функций.

Методология исследования включает:

- анализ нормативно-правовой базы и внутренних регламентов;
- полуструктурированные интервью с оперативным персоналом (12–15 интервью по 40–60 минут);
- обработку статистики инцидентов за 12 месяцев;
- количественную оценку рисков и моделирование сценариев [4, 5, 7].

Достоверность результатов обеспечена триангуляцией данных: сопоставлением формальных регламентов, мнений сотрудников и объективных метрик [9].

На основе анализа документов и интервью выделены следующие группы рисков:

- Операционные риски: задержки реагирования, ошибки передачи информации, нарушение регламентов;
- Технические риски: отказ каналов связи, сбои сигнализации, проблемы с транспортом;
- Кадровые риски: нехватка персонала в пиковые периоды, недостаточная подготовка, текучесть;
- Внешние риски: ложные срабатывания, массовые мероприятия вблизи охраняемых объектов, погодные условия [1, 3].

Интервью с начальниками смен и операторами показали, что наиболее ощутимыми являются риски, связанные с коммуникацией и связью: при потере канала связи время реагирования увеличивается, а координация между группами ухудшается [4].

Для приоритизации рисков использована матрица «вероятность × последствия» [1, 3]. Вероятность определялась на основе статистики инцидентов, последствия оценивались экспертами по шкале 1–5. Уровень риска рассчитывался по формуле:

$$R=P \times I$$

где P - вероятность, I - последствия.

Таблица - Матрица рисков для подразделения вневедомственной охраны (фрагмент)

Риск	Вероятность (P)	Последствия (I)	Уровень риска (R)	Приоритет
Ложное срабатывание, перегрузка смены	0.8	3	2.4	Средний
Пропуск реального	0.1	5	0.5	Низкий (по матрице),

проникновения из-за ошибки оператора				высокий по значимости
Отказ канала связи при выезде группы	0.2	4	0.8	Средний

Несмотря на низкую вероятность, риски с высокими последствиями требуют отдельных мер, поскольку их реализация может привести к критическим последствиям [3, 8].

Для объективной оценки устойчивости рассчитаны следующие метрики:

1. Среднее время реагирования (ART):

$$ART = \sum_{i=1}^n t_i / n$$

где t_i - время реагирования по каждому инциденту, n - количество инцидентов;

2. Доля ложных срабатываний (FAR):

$$FAR = N_{\text{ложн}} / N_{\text{всего}} \times 100\%$$

где $N_{\text{ложн}}$ - количество ложных срабатываний, $N_{\text{всего}}$ - общее количество срабатываний;

3. Коэффициент готовности (GR):

$$GR = T_{\text{раб}} / T_{\text{общ}} \times 100\%$$

где $T_{\text{раб}}$ - время, когда система была полностью готова к реагированию, $T_{\text{общ}}$ - общее время наблюдения [5, 7].

По данным за 12 месяцев (условные значения для примера), среднее время реагирования составило 7,2 минуты, доля ложных срабатываний — 38%, коэффициент готовности — 94%. Высокий процент ложных вызовов создаёт дополнительную нагрузку на дежурные группы и снижает устойчивость системы в пиковые периоды [5].

Таблица 2 - Динамика ключевых метрик устойчивости за 12 месяцев

Месяц	ART, мин	FAR, %	GR, %
1	6,8	35	95
2	7,1	37	94
---	---	---	---
12	7,5	41	93

Тенденция роста FAR и снижения GR в конце периода свидетельствует о нарастании операционных нагрузок и необходимости корректирующих мер [5, 7].

Для проверки устойчивости построены три сценария:

- Best case: все системы работают, связь стабильна, персонал

полностью готов;

- Expected case: типичные проблемы (один ложный вызов, кратковременная потеря связи на 3–5 минут);
- Worst case: одновременный отказ связи, ложные вызовы на нескольких объектах, нехватка экипажей [3, 8].

В worst-case сценарии время реагирования увеличивалось на 40–50%, а доля объектов без прикрытия достигала 15–20%. Это свидетельствует о недостаточной устойчивости системы к каскадным сбоям и необходимости резервирования ресурсов [3, 8]. Разбор учений показал, что при потере связи сотрудники используют резервные каналы и дублирующие маршруты, однако эти процедуры не всегда формализованы и зависят от опыта конкретного начальника смены. Это создаёт риск непоследовательного реагирования в критических ситуациях [6].

С учётом выявленных рисков и результатов моделирования предложены следующие меры:

1. Резервирование каналов связи и дублирование маршрутов. Это снижает риск потери коммуникации и позволяет сохранить управляемость в worst-case сценариях [1, 3];
2. Оптимизация обработки ложных срабатываний. Внедрение алгоритмов предварительной фильтрации и распределение нагрузки между сменами позволит снизить влияние ложных вызовов на устойчивость [5, 7];
3. Формализация процедур на случай сбоев. Разработка чётких инструкций для типовых нештатных ситуаций (потеря связи, нехватка экипажей) и их регулярное обновление на основе разбора инцидентов [6];
4. Регулярные учения и тренировки по сценариям. Моделирование worst-case ситуаций и разбор действий персонала помогут повысить готовность и снизить человеческий фактор [6, 8];
5. Мониторинг и отчётность по метрикам устойчивости. Ежемесячный расчёт ART, FAR и GR позволит своевременно выявлять отклонения и корректировать процессы [5, 7].

Эти меры соответствуют принципам риск-менеджмента по ГОСТ Р ИСО 31000-2019 и адаптированы под специфику вневедомственной охраны [1].

Проведённое исследование показало, что риск-менеджмент является эффективным инструментом повышения устойчивости вневедомственной охраны при условии его практической интеграции в операционные процессы. Использование матрицы рисков, количественных метрик и сценарного моделирования позволяет не только выявлять и приоритизировать риски, но и объективно оценивать устойчивость системы.

Предложенные меры (резервирование каналов связи, формализация процедур, мониторинг метрик, регулярные учения) могут быть внедрены в подразделения вневедомственной охраны с минимальными организационными затратами и способны существенно снизить вероятность критических сбоев.

Дальнейшее развитие темы возможно в направлении разработки

отраслевых методических рекомендаций по риск-менеджменту для охранных структур и создания автоматизированной системы мониторинга устойчивости на базе текущих метрик [1, 3, 5].

Библиографический список

1. ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство». - М.: Стандартинформ, 2019. (дата обращения: 27.07.2026)
2. ISO 31000:2018 «Risk management - Guidelines». (дата обращения: 27.07.2026)
3. Иванов А.А., Петрова М.М. Организационная устойчивость: современные подходы и инструменты // Вестник университета. 2023. № 4. С. 45–58. (дата обращения: 27.07.2026)
4. Смирнов В.К. Методы экспертных оценок и интервью в эмпирических исследованиях // Управленческий учёт. 2022. № 7. С. 112–125. (дата обращения: 27.07.2026)
5. Кузнецов Д.Л. Статистические методы оценки эффективности служб оперативного реагирования // Экономика и управление. 2021. № 12. С. 89–102. (дата обращения: 27.07.2026)
6. Методические рекомендации по организации учений и тренировок в подразделениях охраны. МВД России, 2020. (дата обращения: 27.07.2026)
7. Фёдоров Е.Н. Метрики готовности и оперативности: расчёт и применение в государственных структурах // Менеджмент в России и за рубежом. 2023. № 3. С. 33–44. (дата обращения: 27.07.2026)
8. Харитонова С.В. Сценарное моделирование в управлении устойчивостью инфраструктуры // Стратегическое планирование. 2022. № 5. С. 77–89. (дата обращения: 27.07.2026)
9. Щукин П.Р. Триангуляция данных в эмпирических управленческих исследованиях // Научный журнал. 2021. № 8. С. 22–35. (дата обращения: 27.07.2026)
10. Яковлев О.М. Риск-менеджмент в государственных охранных структурах: специфика и практика // Государственная служба. 2023. № 2. С. 55–67. (дата обращения: 27.07.2026)