

VII. Автоматизированные системы и средства обеспечения безопасности сложных систем

Ничепорчук В.В.

Интеллектуальные сервисы территориального управления безопасностью

Аннотация: Представлена концепция создания интеллектуальных сервисов, автоматизирующих полный цикл решения задач управления безопасностью территорий. Показана универсальность подхода к формированию информационных ресурсов и проектированию процессов их обработки.

Ключевые слова: инструменты формализации, информационные ресурсы, интеллектуальные сервисы, жизненный цикл

Исследования территориальных рисков являются логическим продолжением методов оценок рисков промышленных объектов [1, 2]. Управление объектовыми рисками на основе результатов моделирования различных сценариев реализации опасностей производств включает снижения объемов опасных веществ и материалов, реализацию мероприятий защиты персонала, населения и инфраструктуры. В соответствии с законодательством [3, 4], надзорные органы на основе оценок рисков могут изменять процессы функционирования промышленных объектов (лицензирование, временная остановка, требования по перепрофилированию и т.п.).

Специфика характеристик территорий не позволяет экстраполировать перечисленные подходы на уровень поселений, муниципалитетов, других субъектов оценивания [5]. Поэтому расчеты территориальных рисков носят рекомендательный характер,

эпизодически используются в процессе планирования систем защиты. Отсутствуют требования как к информационным ресурсам, так и методам расчетов.

В работе предлагаются методы перевода методик оценивания территориальных рисков в практику территориального управления. Основной акцент сделан не на повышении детализации и точности вычислений, увеличении номенклатуры показателей и формированию больших временных рядов, а на повышение доверия лиц, принимающих решения, к результатам анализа, использование объяснений процессов получения и трансформации данных.

Задачи управления безопасностью территорий относятся к числу сложных, высокointенсивных, требующих сбора и анализа большого количества разнородных данных, экспертных знаний, а также согласованных действий разных ведомств и уровней управления. Исходя из этого, интеллектуальные сервисы поддержки управления интегрируют следующие информационные ресурсы

$$R = \langle D, K, H \rangle, \quad (1)$$

где D – данные о защищаемых объектах и опасных событиях;

K – знания, включающие явные и неявные знания экспертов, а также правила и ограничения, нормативно-правовых и методических документах;

H – иерархия акторов, принимающих решения на основе разных наборов D и K .

Интеллектуальные сервисы интегрируют BI-инструменты анализа, включая Machine Learning (ML), для обработки и визуализации D ; технологии гибридных экспертных систем для K , H [6, 7]. Хранилища данных позволяют работать с реляционными данными и графовыми представлениями правил, процессов, иерархий, записанных в форматах xml и json.

Однако в современных условиях создание монолитной интеллектуальной системы не представляется возможным. Внедрение альтернативы программных комплексов «Безопасный город», «Система 112», АИУС РСЧС не будет поддержано государственными структурами. Архитектура «монозадачных» микросервисов более адаптивна к разным условиям эксплуатации.

Это могут быть и автономные системы, работающие при неустойчивой связи (Арктика, беспилотная опасность), и агентные модули существующих систем, позволяющие накапливать и распространять знания K о способах и алгоритмах решения задач управления.

Организация данных

Для поддержки планирования и реализации предупредительных (и оперативных) мероприятий необходимо и достаточно информационных ресурсов, содержание которых описывает характеристики защищаемых объектов и имеющихся ресурсах, реестры формирований и каталоги событий (рисунок 1).

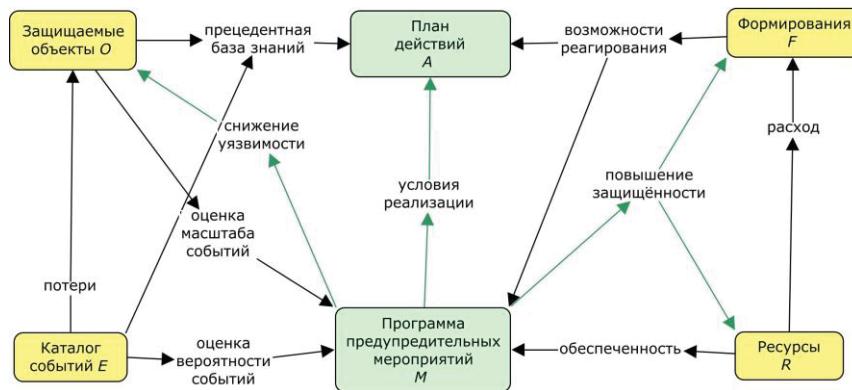


Рисунок 1 – Онтология данных

Технологически структура D представлена элементами: системообразующие ресурсы (справочники и классификаторы), собственно данные об объектах и процессах; репозиторий метаданных; пространственные данные, которые невозможно получить автоматическим геокодированием.

Ориентация информационных ресурсов на один вид ситуации (риска) обуславливает компактность структуры и содержания таблиц. Усложнение предлагаемой структуры также нецелесообразно, поскольку смежные задачи управления, такие как мониторинг обстановки, управление в режиме повышенной

готовности при угрозе чрезвычайных ситуаций (ЧС) можно представить как экземпляр структуры без потерь информативности.

В отличие традиционных методов оценки рисков по каталогам событий, применение ML позволяет объективно кластеризовать территории на основе уязвимости и защищенности. При этом количество кластеров должно соответствовать числу периодов планирования, а размер – объему ресурсов.

Формирование знаний

Стратегическое управление безопасностью территорий представляет собой сложный многоэтапный процесс, в котором задействовано большое количество акторов, описываемых иерархией H [7]. В отличии от учетных систем, информационная поддержка обоснования, планирования реализации превентивных мероприятий требует учета большого числа неопределенных факторов и причинно-следственных связей. Переход к управлению на основе данных включает изменение бизнес-процессов и функций органов управления, повышение зрелости используемых данных, создающих условия для внедрения и успешной эксплуатации.

Интеллектуальный сервис предназначен для формирования решений путем поиска аналогов в паттернах (базы типовых решений) на основе метрики ситуации, получаемой по результатам многопараметрического анализа показателей ситуации. В терминах О.А. Николайчук [8] решение формируется как повторное использование опыта и технологии рассуждений по аналогии (case-based reasoning). Решения формируются на основе интеграции предметной базы знаний и прецедентной модели

В рамках пилотной реализации интеллектуальных сервисов formalизованы задачи противопожарной защиты сельских территорий, включающие создание новых или кардинальное изменение характеристик формирований, водоисточников, процессов подготовки к весенне-летнему пожароопасному сезону. Процесс formalизации документов, а также неявных знаний экспертов показал необходимость разработки двух алгоритмов – для самостоятельных в бюджетном отношении территорий с меньшим количеством элементов H , и дотационных, где в процесс принятия решений включены надзорные и контрольные органы управления.

Простота понимания процессов решения задач управления, переход от слабо формализованных рассуждений к алгоритмам и математической постановке достигается через графические представления состояний объектов и процессов их изменения, включая нотации IDEFx, BPMN, UML, Arhcimate, DMN, онтологии, сети Петри и другие. Перечисленные нотации обладают разной степенью формализма и взаимодополняют друг друга. Совместное использование приводит к некоторой избыточности описания, но позволяет раскрыть разные аспекты проблемы.

Заключение

Предлагаемый подход разработан для решения «монозадач» достаточного большого объема, но с равным информационным обеспечением всех акторов иерархии управления, принимающих решения. При этом реализуется информационное сопровождение полного жизненного цикла объектов управления: создание, мониторинг состояния, эксплуатация, списание. Это устраняет существующий дисбаланс управления, сочетающий комплексный мониторинг обстановки, адекватные модели ситуаций с плохо проработанными планами действий по предупреждению и ликвидации ЧС.

Внедрение интеллектуальных сервисов, реализующих полный цикл управления, позволит повысить достоверность информации для принятия решений, снизить трудоемкость решения задач управления территориальной безопасностью. Машиночитаемые представления всех информационных ресурсов обеспечивают их достоверность путем применения статистических и логических методов верификации.

Изменение бизнес-процессов включает исключение операций агрегирования и ручного формирования отчетов. Вместо этого используют BI-инструменты, позволяющие настраивать представления данных и вычислительные методы под конкретную задачу. В условиях роста объемов информации необходимы сервисы работы с решениями, включая функции их формализации, проверки, хранения, поиска аналогов и формирования для конкретных ситуаций. Это позволит экспертам и лицам, принимающим решения (ЛПР) минимизировать затраты на восприятие и понимание

ситуации, сосредоточиться на анализе альтернатив и обосновании оптимальных решений.

Неотъемлемой частью интеллектуальных сервисов является интерфейс оперативной трассировки и верификации машинных решений. Главная цель информационной поддержки задач управления безопасностью территорий – уменьшение числа ошибочных решений, приводящих к огромным потерям. Оценить количественно экономический эффект внедрения интеллектуальных сервисов затруднительно. Однако многолетние исследования процессов подготовки решений в МЧС России и других органов управления показывают возможности исключения рутинных операций по обработки данных, повышение их зрелости уже на этапе формирования. Создание и распространение знаний в увязке с потребностями ЛПР повысит качество управления, а, следовательно, уровень безопасности населения и инфраструктуры в условиях ограниченных ресурсов и роста негативных факторов природного и техногенного характера.

*Работа выполнена в рамках государственного задания
ФИЦ КНЦ СО РАН программы фундаментальных исследований
Российской Федерации (рег. FWES-2021-0004)*

Литература:

1. Пенькова Т.Г., Метус А.М., Ничепорчук В.В. Метод интегрального аналитического оценивания природно-техногенной безопасности территорий (на примере Красноярского края) // Проблемы анализа риска. – 2018. – Т. 15, № 5. – С. 16-25. – DOI: 10.32686/1812-5220-2018-15-5-16-25.
2. Быков А.А., Зайковский В.Э. Методологические и прикладные основы управления рисками предприятия и безопасностью населения и окружающей среды. – Томск : Издательство ТУСУРа, 2022. – 616 с.
3. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2020. – 19 с.
4. Федеральный закон от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности». – URL: <https://www.garant.ru/products/ipo/prime/doc/402707588> (дата обращения 19.09.2025).

5. Гаврилова Т.А., Хорошевский В.Ф. Базы знаний интеллектуальных систем. – СПб.: Питер, 2000 – 384 с.
6. Колесников А.В., Кириков И.А. Методология и технология решения сложных задач методами функциональных гибридных интеллектуальных систем. – М.: ИПИ РАН, 2007. – 387 с.
7. Ничепорчук В.В. Исследование информационной обеспеченности взаимодействия в РСЧС // Технологии гражданской безопасности. – 2024. – Т. 21, № 4 (82). – С. 43-47.
8. Николайчук О.А., Юрин А.Ю. Управление опытом при исследовании динамики технического состояния уникальных машин и конструкций: моделирование опыта // Информационные технологии. – 2008. – №6 – С. 30-37.

Сиротюк В.О., Богатырева Л.В.

Комплексная безопасность субъектов системы управления интеллектуальной собственностью

Аннотация: Проведен анализ предпосылок создания комплексной системы информационной безопасности организаций-субъектов системы управления интеллектуальной собственностью (ИС) в современных условиях. Рассмотрены характеристики и особенности построения объектов безопасности системы управления ИС, требования по обеспечению их нормального функционирования. Сформулированы цели и задачи комплексной системы безопасности субъектов ИС. Разработаны мероприятия по построению комплексной системы безопасности информационной и обеспечивающей инфраструктуры субъектов ИС, цифрового патентного информационного фонда ИС. Предложенные методы и мероприятия использовались при построении эффективной комплексной системы безопасности региональной патентной организации.

Ключевые слова: система управления интеллектуальной собственностью, организаций-субъекты интеллектуальной собственности, цифровой информационный фонд