



Рыбак Александр Владимирович, заместитель начальника кафедры информационного и технического обеспечения ОВД Дальневосточного юридического института МВД России, к.т.н., доцент, полковник полиции



Дунин Вадим Сергеевич, преподаватель кафедры информационного и технического обеспечения ОВД Дальневосточного юридического института МВД России, майор полиции

В рамках Концепции информатизации ОВД, а также типового проекта (модели) по созданию правоохранительного сегмента обеспечения правопорядка и безопасности в 2010 г. в г. Хабаровске была разработана и внедрена комплексная автоматизированная информационно-аналитическая система (КАИАС) «Безопасный город», в которую вошли десять подсистем функционирования (рис. 1):

Развитие комплексной автоматизированной информационно-аналитической системы «Безопасный город» на примере интеграции в единую среду межведомственного взаимодействия: проблемы и пути решения в Хабаровском крае

- телекоммуникационная инфраструктура ИМТС ОВД;
- подсистема видеонаблюдения, обработки и хранения видеoinформации;
- подсистема приема сообщений о происшествиях;
- подсистема управления и поддержки принятия решений;
- подсистема мониторинга и управления мобильными объектами;
- подсистема интеграции с внешними навигационными системами;
- геоинформационная подсистема отображения интерактивной карты города с возможностью нанесения нескольких слоев с данными;
- подсистема связи (проводной и радиосвязи);
- подсистема взаимодействия с внешними источниками данных;
- подсистема обеспечения комплексной безопасности.

Основной целью развертывания аппаратно-программного комплекса системы в г. Хабаровске было повышение процесса подготовки и принятия решений в деятельности органов внутренних дел и переход на качественно новый функциональный уровень взаимодействия между подразделениями. Но, к сожалению, как показывает практика, полностью эту цель реализовать не удалось.

Прежде всего, обращает на себя внимание следующие тревожные факторы:

- низкий коэффициент полезного действия КАИАС «Безопасный город». Большая часть полезной ин-

формации, предоставляемая системой, не находит применения либо из-за низкого профессионализма операторов (отсутствие знаний об интеллектуальных возможностях системы), либо из-за отсутствия профессионального интереса;

- средняя работоспособность оборудования КАИАС (в настоящий момент до 30% всех камер подсистемы видеонаблюдения не в активном режиме), динамика отказов оборудования положительная;
- отсутствие необходимой модернизации из-за перехода органов внутренних дел на финансирование из федерального бюджета и невозможности прямого получения денежных средств из краевого и муниципального бюджетов.

Все это, безусловно, не только не позволяет эффективно использовать КАИАС «Безопасный город» в правоохранительной деятельности, но и свидетельствует об отсутствии всякой перспективы ее развития уже в ближайшем будущем.

Сотрудниками кафедры информационного и технического обеспечения ОВД ДВЮИ МВД России совместно со специалистами ООО ДСЦБИ «МАСКОМ» была изучена сложившаяся ситуация и выявлены основные проблемы, решения которых, к сожалению, лежат за пределами возможностей Министерства внутренних дел и требует подключения других ведомств. Эти проблемы заключаются в следующем.



Рис. 1. Состав подсистем функционирования КАИАС «Безопасный город» УМВД России по г. Хабаровску

1. Отсутствует целенаправленное программное финансирование со стороны всех (четырех, в том числе частного) бюджетных уровней. Сегодняшняя разобщенность структур, решающих задачи обеспечения безопасности жизнедеятельности, приводит к тому, что инвестиции на их технологическое оснащение «зарываются» в создание изолированных систем, слабо увязанных по задачам и протоколам информационного взаимодействия и требующих чрезмерных затрат на разработку, внедрение и сопровождение. Кроме того, обширные территории Российской Федерации, низкая плотность населения в регионах значительно увеличивают удельную стоимость объектов информационной инфраструктуры, делая их создание в интересах отдельного ведомства нерентабельным и неоправданно дорогим.

2. Отсутствует квалифицированный персонал.

Например, сами по себе системы видеонаблюдения не являются источниками оперативной информации без связи с человеком – высококвалифицированным оператором, а ввиду необходимости задействования (в охране общественного порядка) большого количества камер может потребоваться соответствующее количество операторов. В то же время при отсутствии высококвалифицированного персонала, эффективно использующего системы видеоконтроля в реальном времени (с учетом применения интеллектуальных камер и систем распознавания образов), система видеонаблюдения продолжает функционировать в режиме источника видеозаписей, по которым (впоследствии) имеется возможность восстановления истории события, но и этот раздел информации (как правило) оста-

ется недоступным для заинтересованных подразделений.

3. Отсутствует законодательно утвержденная возможность (регламент) использования информационно-технологических ресурсов других ведомств.

Например, автоматические системы фиксации нарушений ПДД позволяют с высокой степенью эффективности «заменить» сотрудников ДПС, при этом качественно решая задачи обеспечения безопасности на дорогах. Вместе с тем указанные системы являются источниками побочной информации об интенсивности движения, фактах проезда разыскиваемого автотранспорта (в том числе установления маршрута движения угнанного автомобиля). Имеющиеся в системах фиксации нарушений ПДД данные можно было бы использовать в интересах других ведомств и подразделений УМВД России по Хабаровскому краю, например службы судебных приставов, оперативных служб розыска автотранспорта, предприятий, ответственных за организацию дорожного движения, и т.д.

Отсутствие регламентов межведомственного взаимодействия приводит к тому, что процесс обмена данными между владельцами и потребителями этих информационных ресурсов усложняется. Поэтому на первый план выступают задачи развития информационно-телекоммуникационной инфраструктуры и организации юридически значимого защищенного межведомственного информационного взаимодействия.

4. Отсутствует возможность обеспечения стабильности работы системы.

Данная проблема касается всего комплекса технических средств, включенных в КАИАС – как ведомствен-

ных, так и вневедомственных. Обеспечение бесперебойной работы и постоянного сопровождения эксплуатации КАИАС невозможно в условиях:

- отсутствия распределения прав, обязанностей, функций и т.д. между владельцами (ведомствами, подразделениями, предприятиями) различных систем обеспечения безопасности, включенных в КАИАС «Безопасный город»;

- отсутствия квалифицированных технических (инженерных) сотрудников (штатных / не штатных);
- отсутствия комплексных обслуживающих бригад из-за большого географического размера системы;
- отсутствие у лиц, принимающих решения, понимания того, что КАИАС «Безопасный город» — это не комплекс видеоконтроля мест массового пребывания граждан, а интегрированная в ведомственную информационную среду комплексная система обеспечения безопасности объектов инфраструктуры и жизнедеятельности граждан.

По своей сути комплекс различных датчиков КАИАС «Безопасный город» является лишь источником информации, которая служит для наиболее полного определения событий о правонарушениях и преступлениях.

Еще одним важным аспектом использования в правоохранительной деятельности функций системы является реакция (как самой КАИАС, так и её операторов) на детектирование событий, контроль исполнения всех функций, фиксация фактов и сохранение их в архиве для последующего анализа и т.д. Этот аспект требует обязательного наличия в системе подсистем: автоматизированного управления, мониторинга сил и средств, современной цифровой подвижной и фиксированной связи, поддержки принятия решения, прогнозирования развития ситуаций. Указанные подсистемы должны присутствовать на всех уровнях оперативного контроля и управления обеспечения безопасности микрорайона, города, субъекта, федерального округа.

Данные подсистемы позволяют осуществлять оперативный контроль обстановки снизу вверх, качественно оценивать деятельность сотрудников.

Направления и пути кардинального решения проблем

Ключевым подходом к кардинальному решению вышеуказанных проблем является системный подход к разработке, реализации и сопрово-

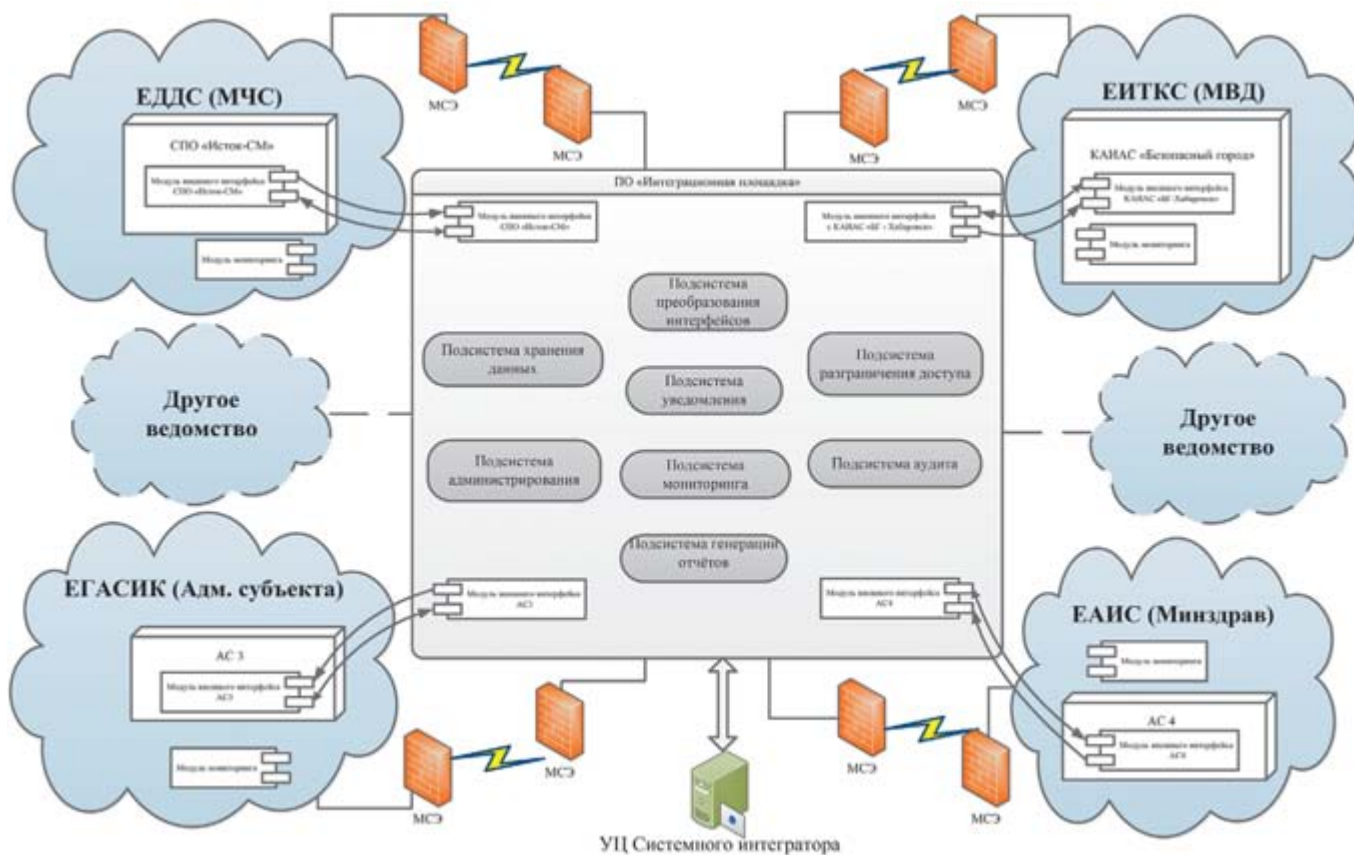


Рис. 2. Примерная схема организации системы межведомственного взаимодействия участников обеспечения безопасности жизнедеятельности субъекта

ждению программ внедрения автоматизированных систем. Учитывая опыт внедрения КАИАС «Безопасный город» в России и за рубежом, необходимость применения этого подхода к решению задач правоохранительных органов назрела и требует решения как минимум в четырех аспектах данной темы.

1. **Управленческий аспект.** Разработка принципов межуровневого, межбюджетного и межведомственного взаимодействия исполнительных органов федеральной и региональной власти, а также органов местного самоуправления. В качестве первого шага целесообразно под эгидой Дальневосточного юридического института МВД России провести «Круглый стол» с приглашением практических специалистов всех заинтересованных ведомств.

2. **Нормативно-правовой аспект.** Разработка новой и доработка существующей нормативной базы федерального, регионального и муниципального уровней. Для решения этой задачи следует создать рабочую группу, куда должны войти не только ученые, но и практические специалисты заинтересованных ведомств.

3. **Кадровый аспект.** Подготовка и обучение специалистов, способных эффективно работать с подсистемами КАИАС «Безопасный город». Для этого потребуются современные полигоны (тренажеры), где можно было бы поставить на поток процесс обучения. В Хабаровском крае на сегодняшний день только ДВЮИ МВД России обладает такой площадкой, где разворачивается многофункциональной информационно-аналитический центр, включающий учебную модель системы.

4. **Технический аспект.** Этот аспект указывает на необходимость применения современных технических средств в расчете на настоящее состояние технологий и перспективного развития с учетом тенденций их совершенствования в мире.

Одна из них — это возможность создания системы межведомственного взаимодействия (СМВ) на существующих технологических площадках специализированных операторов связи (далее — оператор), использующих интеграционные платформы (рис. 2). Предлагая такую схему, оператор в процессе информационного обмена будет являться доверенной тре-

тей стороной. Это означает то, что на серверах оператора не будет храниться передаваемая информация в открытом виде, а будет осуществляться всего лишь контроль, гарантия доставки сообщений и аудит действий, произведенных в системе в зашифрованном виде. Доступ к информации и возможность ее расшифровки в случае необходимости и разрешения споров при конфликтных информационных взаимодействиях будет иметь только уполномоченное лицо заказчика (например, сотрудник подразделения УМВД). Подобная гарантия достигается путем использования технологии электронной подписи.

Указанный подход позволяет более согласованно решать проблемы информационного обмена между конкретными подразделениями и ведомствами, предоставляет возможность расширять существующую систему, создавая новые сценарии взаимодействия с перспективой формирования единого информационного пространства всех участников обеспечения безопасности жизнедеятельности субъекта.