Блок «Координация работы служб и ведомств»

Это ключевой по значению и функционалу блок АПК «Безопасный город» муниципального уровня, который представляет собой Единый центр оперативного реагирования (ЕЦОР, но иногда даже сами региональные координаторы АПК по привычке называют его ЕДДС). Основой ЕЦОР являются интеграционные платформы, которых сейчас в России внедряется несколько, и не факт, что это плохо.

В состав ключевого блока входят всего два сегмента.

1. Единый центр оперативного реагирования (ЕЦОР), имеющий в своем составе:
- подсистему приема и обработки обращений;
- подсистему поддержки принятия решений;
- подсистему комплексного мониторинга;
- интернет-портал;
- подсистему обеспечения координации и взаимодействия;
- подсистему комплексного информирования и оповещения;
- подсистему интеграции данных.

Блок «Координация работы служб и ведомств» представляет собой Единый центр оперативного реагирования, основой которого являются интеграционные платформы

2. Региональная интеграционная платформа в составе:
- модуля ведения реестра комплексов средств автоматизации (КСА) федеральных и региональных систем в сфере обеспечения общественной безопасности, правопорядка и безопасности среды, а также взаимодействующих с ними КСА всех муниципальных образований, входящих в состав региона;
- модуля управления данными.

ЕЦОР должен обеспечивать:

1. Централизованный мониторинг угроз общественной безопасности, правопорядка и безопасности среды обитания:
- прием и регистрацию сообщений об угрозах по доступным в муниципальном образовании каналам связи, включая телефонную связь, интернет, средства экстренной связи;
- комплексный мониторинг угроз, полученных от всех КСА АПК «Безопасный город» (существующих и перспективных) по Единому стеку открытых протоколов.

2. Поддержку принятия решений:
- категоризацию событий и соответствующих им правил реагирования для экстренных оперативных и муниципальных служб;
- автоматическое предоставление вариантов сценария реагирования;
- моделирование различных сценариев возникновения потенциальных угроз безопасности, включая построение прогнозов их развития и отображение на электронной карте результатов моделирования.

3. Управление и координацию взаимодействия:
- обеспечение доступа к единой информационной среде, включая доступ к реестровой, справочной и пространственной информации об объектах инженерной, транспортной и социальной инфраструктуры;
- формирование в автоматическом или полуавтоматическом режиме поручений;
- обеспечение оперативного информирования о статусе события и поручениях служб оперативного реагирования и муниципальных служб, отвечающих за проведение работы над инцидентом;
- управление поручениями и контроль исполнения поручений;
- отображение на электронной карте полной информации о событии, включая просмотр изменения статусов события и выданных поручений.

4. Информирование и оповещение населения муниципального образования:
- комплексное оповещение населения об угрозах безопасности с использованием средств информирования и связи, в том числе громкоговорителей, информационных табло, sms-рассылок, мобильных приложений, электронной почты, радио и телевидения, интернет-портала и иных средств информирования;
- информирование населения о результатах реагирования на угрозы.

5. Формирование единого информационного пространства:
- обеспечение интеграции и информационного взаимодействия между КСА сегментов «Безопасный город» на базе муниципальной и региональной интеграционных платформ;
- обеспечение защищенного доступа к информации с использованием средств криптографической защиты;
- автоматическое архивирование и обеспечение хранения видеоинформации и отчетной информации о событиях и всей сопутствующей информации и т. д.

Подробные требования к ЕЦОР вынесены за рамки ЕТТ и представлены в Приложениях № 3 и № 4.

ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ

Один из главных вопросов при построении систем такого масштаба, как «Безопасный город», — как будут взаимодействовать между собой его подсистемы. Они разрозненны, принадлежат разным ведомствам, создавались по совершенно не связанным между собой техническим требованиям, их владельцы зачастую даже не знакомы друг с другом, не говоря уже о предоставлении доступа к комплексным системам автоматизации своих земляков.

Например, Росморречфлот потратил на оснащение системами безопасности всех портов и гидросооружений около 40 млрд рублей. В результате в России создана отраслевая система безопасности, которая при помощи видеонаблюдения, радаров, тепловизоров обеспечивает такой уровень охраны и защиты объектов, который никто в мире не делает. Однако таможенники, пограничники, другие службы не то что не имеют к этой системе доступа, но даже не знают о ее существовании. И так везде.

Концепция АПК «Безопасный город» подразумевает объединение информации, которая генерируется разрозненными системами, в некую общую среду, где любые данные могут быть использованы для обеспечения безопасности жизнедеятельности населения субъекта РФ.

За обеспечение взаимодействия отвечает ЕЦОР. При этом в ЕТТ установлены требования к характеристикам взаимосвязи систем — они должны либо соответствовать этим требованиям, либо владельцу системы придется за свой счет обновлять ПО или создавать интеграционный шлюз.

Взаимосвязь подсистем внутри АПК «Безопасный город» может быть выполнена только по требованиям Единого стандарта открытых протоколов (ЕСОП). Единый стандарт был разработан после того, как интеграторы «Безопасного города» столкнулись в регионах с нежеланием разработчиков систем предоставлять закрытые протоколы для обеспечения взаимодействия с платформой ЕЦОР. Так произошло, например, в Пензе, где установлена система видеонаблюдения российской разработки, имеющая закрытые протоколы.

Поскольку основные проблемы возникли в первую очередь с интеграцией систем видеонаблюдения, спецификации ЕСОП описывают преимущественно этот сегмент.

По данным заместителя директора центра ЗАО «НПП ИСТА-Системс» к.т.н. Геннадия Кузнецова, который входит в состав экспертного совета по АПК «Безопасный город», в части взаимодействия со средствами формирования и обработки видеоданных протокол основан на спецификациях отраслевого стандарта ONVIF версии не ниже 2.4. Кроме того, в ЕТТ содержится требование дополнить ONVIF при описании видеоисточников спецификациями web-сервисов, описывающими метаданные и правила доступа к видеоисточникам, а именно:

- содержащими сведения о видеоисточниках, в том числе об их географическом местоположении и областях обзора;
- реализующими импорт медиазаписей в форме файлов, в том числе с привязкой к географическим координатам места записи как для стационарных, так и движущихся источников (геотреки);
- реализующими ограничение доступа к видеоисточникам с разбивкой по типу взаимодействия;
- позволяющими управлять заданиями при выполнении длительных операций (например, отслеживание транспортных средств по регистрационному номеру и т. п.).

Однако этих спецификаций недостаточно для систем — источников тревожных сообщений и метаданных — мониторинга безопасности жизнедеятельности, безопасности дорожного движения, экстренной связи «гражданин–полиция», технологических систем контроля оборудования и процессов и других. В частности, в ЕСОП нет механизмов описания уровня угрозы, вероятности ее возникновения, способа реагирования, не предусмотрена передача подробной текстуальной, географической информации, не определены коды ситуаций, общие справочники и многое другое.

В результате экспертный совет при разработке концепции и ЕТТ принял существующий на тот момент так называемый «Протокол МВД», который предусматривает создание систем видеонаблюдения на основе ONVIF, дополненного описаниями метаданных видеоисточников и правилами доступа к ним, а для задач мониторинга и оповещения использует собственный единый стандартизированный протокол извещений (ЕСПИ), основанный на Common Alerting Protocol (CAP) версии 1.2.

Таким образом, проблема с подсистемами, использующими закрытые протоколы, должна быть снята. Правда, заказчикам придется как-то договариваться с исполнителями, которые уже выполнили работу и получили гешефт.

По поводу закрытых или проприетарных протоколов обмена и интерфейсов взаимодействия в ЕТТ стоит лаконичное «недопустимо».

Фото: ©Depositphotos/welcomia

ГОСТ из шести пунктов и обращение к соотечественникам

По словам Владимира Куделькина, президента консорциума «Интегра-С», члена экспертного совета по АПК «Безопасный город» и председателя ТК-125, стандарту по интеграции скоро присвоят номер.

Суть Единых стандартов создания интегрированных интеллектуальных систем безопасности объектов и территории государства сводится к шести пунктам.

1. Использование в интегрированных системах открытых кодов.
2. Использование в интегрированных системах открытых протоколов.
3. Отображение объектов и территорий в 3D-графике.
4. Полицентрическая система распространения информации.
5. Шифрация степеней секретности.
6. Право доступа только через электронную подпись — самую надежную систему защиты информации.

Как считает Владимир Куделькин, этот стандарт разработан не в интересах конкретной компании, а из соображений целесообразности и здравого смысла, поэтому может считаться универсальным для интегрированных систем безопасности объектов и территорий, к которым относится АПК «Безопасный город».

При этом глава «Интегра-С» готов пойти на беспрецедентные меры, а именно — бесплатно заменить всем желающим Microsoft-ориентированное ПО на аналогичное, написанное на открытых кодах.

Уважаемые коллеги-соотечественники!

Информационная система России все больше попадает в кабальную зависимость от вредоносных программ и шпионских web-сервисов.

Уклонение участников ИТ-сообщества и пользователей бюджетной сферы от исполнения действующих нормативных государственных документов приводит к глубокому проникновению в промышленный и служебный оборот программного обеспечения (ПО), разработанного и реализуемого с использованием закрытых исходных кодов. Засилье таким ПО в стране достигает 97%. Эти программы целенаправленно созданы для нанесения ущерба и вреда их пользователям. Массовое применение этого ПО ставит под угрозу безопасность информационного пространства страны и делает национальную экономику и безопасность страны уязвимыми от политического настроения поставщиков и «модераторов» такого ПО.

В мировой практике процессы импортозамещения и ухода от вредоносного ПО ускорились… Пример кардинального подхода демонстрирует Китай, где на правительственном уровне решено заменять в год до 15% ОС Windows на Linux. В Германии более 65% коммерческих компаний использует свободное ПО, во Франции — 67%, в Финляндии на СПО перешло более 80% частных компаний (National Open Source, Software Observatory).

В этих условиях нами принято решение, что впредь все разрабатываемые и устанавливаемые программные продукты нашего консорциума будут содержать только открытые исходные коды (Linux) и использовать только открытые протоколы.

Для ускорения процесса перехода на Linux начиная с 11 января 2016 года мы готовы для замены ранее поставленной и используемой программной продукции под Windows бесплатно предоставить необходимые программные продукты под Linux.

Для компаний, не являющихся нашими клиентами (имеющих ПО, установленное начиная с 2005 г.), мы готовы также без оплаты, после проработки технической возможности предоставить необходимое программное обеспечение.

Последовать нашему примеру мы призываем и других участников рынка информационно-коммуникационных технологий.

Пора сплотиться в борьбе за безопасное государство и вести ее по правилам, исключающим применение нечестных приемов, запрещенных ударов и недекларированных возможностей.

Надеемся на ваше понимание, дальновидность и искренний патриотизм!

Обращение консорциума «Интегра-С» к участникам рынка информационно-коммуникационных технологий. Полный текст обращения опубликован на сайте компании.