«ЦИФРОВОЙ ПОЛИЦЕЙСКИЙ»

Гао Хоронг, эксперт по решениям проблем обеспечения общественной безопасности компании «Huawei»

Реализация ИКТ-проектов в сфере обеспечения безопасности: искусственный интеллект

В 2016-м компания Huawei была среди пионеров обоснования необходимости цифровой трансформации агентств, служб, обеспечивающих общественную безопасности, концепции Объединенной общественной безопасность. В сущности, из-за развивающихся угроз общественной безопасности и оперативных задач силовые структуры успешно могут бороться комплексно и преодолевают проблемы самостоятельно. Но ситуация меняется. Службы, даже на уровне городов и стран, нуждаются в более тесном сотрудничестве. Последние инновационные технологии позволяют внедрять новые процессы и сервисы для более эффективного обеспечения правопорядка. Важно то, что, как в случае цифровизации экономики, структурам обеспечения правопорядка необходимо использовать платформы для взаимодействия с сообществами и сотрудничать с ними в предотвращении, обнаружении, реагировании и восстановлении после угроз. В 2017 году Huawei запустил комплекс решений «C-C4ISR» для обеспечения работы Объединенной общественной безопасности.

Отрадно видеть, что в последнее время все больше консалтинговых и технологических компаний и даже органов общественной безопасности пропагандируют цифровую трансформацию общественной безопасности. С другой стороны, угрозы безопасности эволюционируют и нарастают лавинообразно, усугубляя текущие операционные проблемы. В качестве примеров:

Образованные люди агитируются в on-line пространстве в поддержку терроризма и радикализма.

Использование БПЛА для контрабанды наркотических средств и дронов для покушения на жизнь президента Венесуэлы.

Использование популярных on-line сервисов и игр для воздействия на детей или размещение запрещенных изображений внутри blockchain.

Критичные недостатки в безопасности популярного промышленного программного обеспечения ставят под угрозу электросети.

Службы по-прежнему не обмениваются критически важной информацией.

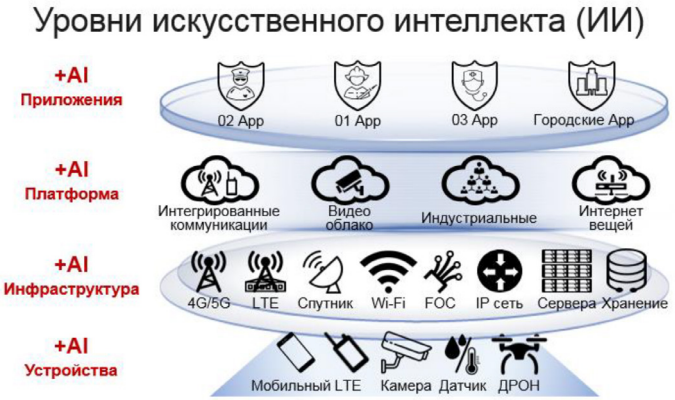
Преступники все чаще обходят системы распознавания лиц.

Устаревшие технологии являются проблемой при координации работ.

Цифровая трансформация может казаться роскошной и недостижимой многим структурам. Но с учетом изменений, описанных выше, выбор стоит между трансформацией или цифровым крахом. Структуры, обеспечивающие безопасность населения, должны ускориться в принятии Объединенной общественной безопасности. Даже вновь создаваемые структуры без ранее реализованных технологических проектов могут воспользоваться цифровой трансформацией. Конечно, такие структуры имеют преимущество даже перед скачкообразно развивающимися организациями, использующими ранее реализованные технологии.

Является ли искусственный интеллект (ИИ) способом ускорения цифровой трансформации общественной безопасности? Короткий ответ: да. Но на пути слишком много искажений и путаницы, которые надо преодолеть для получения пользы от внедрения ИИ. Из почти тридцатилетнего опыта в обеспечении безопасности населения от патрульного офицера до разработчика технологических решений обеспечения общественной безопасности я сделал вывод, что и для незаурядных организаций затруднительно быстро внедрить самые новые технологические видения. Например, компания-разработчик программного обеспечения быстро меняет технологии: бизнес-аналитику на систему поддержки принятия решений, далее на визуальную аналитику, большие данные и ИИ. Почти все компании видеоаналитики позиционируют себя как компании внедрения искусственного интеллекта. Значит ли это, что перечисленные технологии могут быть заменены так быстро?

Для того чтобы внедрение Искусственного интеллекта было выполнимым и выгодным, нужно смотреть под разными углами на проблематику, начиная с базового. Во-первых, с технологической стороны мы должны понимать, что ИИ может быть использован на различных технологических уровнях:



Позвольте объяснить возможности искусственного интеллекта на некоторых уровнях и компонентах через данный сценарий:

Гражданин стал свидетелем ограбления банка и видел грабителя, убежавшего с пистолетом. Он набрал телефон службы спасения и сообщил о преступлении. Компьютерная система диспетчеризации, промышленная реализация приложения и интегрированная коммуникационная платформа, обе использующие элементы искусственного интеллекта, смогли принять звонок и запросить необходимую информацию самостоятельно, без участия оператора.

Эта же система и платформа способна распределить автоматически задачу на доступного сотрудника в районе места происшествия и направить его для поиска грабителя

Один офицер поблизости увидел подозреваемого, и последний выстрелил в офицера. Офицер начал преследование. ИИ активировал интеллектуальное видеонаблюдение на основе носимого eLTE устройства, которое направило сигнал тревоги в командный центр, и другие сотрудники в районе происшествия получили команду участвовать в погоне.

На инфраструктурном уровне сеть eLTE способна обеспечить приоритет устройствам сотрудников для гарантированного обеспечения связи.

Используя информацию о местоположении сотрудников, получаемую в режиме on-line, ИИ активирует сеть видеонаблюдения, направляя камеры в предполагаемую сторону сотрудника и подозреваемого для сбора видеопотока в высоком разрешении.

На уровне платформы видео облако способно выстроить траекторию движения подозреваемого и даже прогнозировать направление дальнейшего движения.

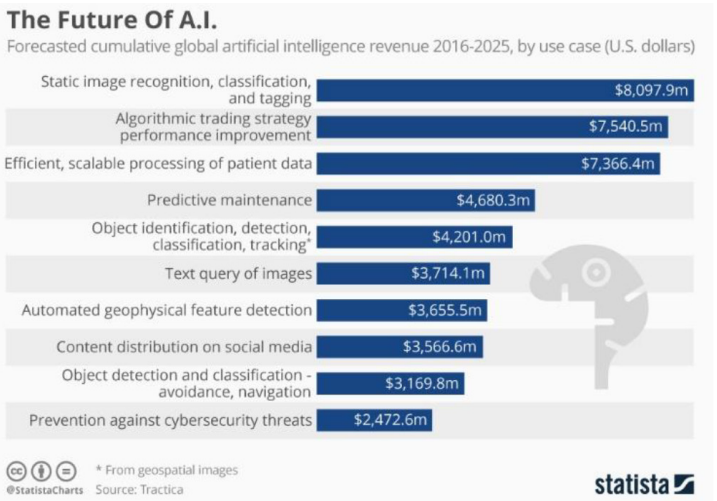
Другое приложение, запущенное на платформе приложений, в автоматическом режиме запускает БПЛА для перехвата подозреваемого и направляет видео реального времени в командный центр и участвующим в погоне сотрудникам.

Автономно БПЛА посылает запрос для опознавания снимаемого подозреваемого

Примеры использования ИИ в Общественной безопасности - Семь А.

Выше изложен только один из множества возможных сценариев использования искусственного интеллекта. Как любое технологическое внедрение, необходимо начинать с проблемы, которую мы хотим решить или результата, которого хотим добиться. В Интернете каждый из нас может найти множество статей об использовании ИИ для обеспечения безопасности населения, но это в основном описание перспектив. Единственным общим знаменателем для различных структур, обеспечивающих правопорядок, особенно в разных странах, является их миссия. Очень часто законы наделяют их разными полномочиями, их структуры, процедуры, люди, технологии, бюджеты - различны.

То, что нам нужно, это категоризация и руководство для служб общественной безопасности, чтобы обратиться к ним, чтобы планировать свои внедрения ИИ в будущем. На эту тему мы вновь можем найти множество исследований в Интернете, повествующих о «горячих» случаях использования ИИ. Один из полезных отчетов, тем более что автор указал «ценник» на каждый из примеров,- «Будущее искусственного интеллекта» Мартина Армстронга:



Хотя использованные примеры относятся ко всем индустриям, примечательно, что 8 из 10 относятся к общественной безопасности:

1.Распознавание статичных изображений, классификация и маркировка: С увеличением количества фотографий / видео из социальных сетей и камер наблюдения такой анализ и маркировка имеют решающее значение в решении и даже предотвращении незаконных действий.

2.Предиктивное обслуживание: Службы обеспечения безопасности используют большое количество логистических услуг для перевозки от оружия до специальных средств спасения. Такое превентивное обслуживание технических средств вполне применимо.

3.Идентификация, обнаружение, классификация, отслеживание объектов: Аналогично статичным изображениям, распознавание, упомянутое выше, в режиме реального времени, анализ и отслеживание перемещения предмета имеет даже более критичное значение. Объект может быть человеком, мобильным телефоном, украденным имуществом, транспортным средством, оружием или даже бомбой.

4.Текстовый запрос изображений: Будь то поиск после события или анализ больших данных до события, необходимость преобразования изображений в текстовые данные важна на протяжении всего жизненного цикла общественной безопасности, а именно предотвращения, обнаружения, реагирования и восстановления.

5.Автоматическое обнаружение геофизических объектов: Четыре важных сущности общественной безопасности - это люди, объекты, места и события. Будь то словесное описание жертвой местоположения или доказательства, найденные в киберпространстве, геофизическая идентификация станет большим подспорьем.

6.Распространение контента в социальных сетях: В соответствии с концепцией Совместной общественной безопасности сотрудничество с сообществами осуществляется не только в физическом мире, но и через социальные сети. Учреждения должны завоевать доверие населения, прежде чем использовать их для совместного обеспечения общественной безопасности.

7.Обнаружение и классификация объектов - предотвращение, навигация: Это актуально, когда органы общественной безопасности начинают использовать дроны и даже роботов.

8.Предотвращение угроз кибербезопасности: Хотя это относится ко всем отраслям, особенно важно для общественной безопасности, во-первых, для служб, чтобы защитить свои очень конфиденциальные данные, а во-вторых, для снижения киберпреступности.

В то время как приведенный выше список случаев использования является довольно полным на данный момент, считаю, что нам нужно включить три других слу-

чая использования ИИ в общественной безопасности:

1.Язык и звуковая обработка: От автоматического принятия вызова до законного перехвата связи, такая возможность важна для общественной безопасности.

2.Планирование: От предупреждения преступлений до обеспечения безопасности крупных событий, от управления при ликвидации чрезвычайных ситуаций до расследования после событий органам общественной безопасности необходимо планирование мобилизации и развертывания ресурсов.

3.Анализ: Лучший способ предотвратить преступление - понять, когда, где и почему произошли прошлые преступления. Возможность анализа будет полезна.

Несмотря на полноту, приведенные выше примеры использования ИИ в значительной степени обусловлены технологическими возможностями. Что нам нужно, так это общая структура практических примеров использования для различных служб, обеспечивающих общественную безопасность, чтобы разработать дорожную карту внедрения ИИ на основе существующего законодательства, организационной структуры, действующих процедур, внедренных ранее технологий и доступных бюджетов, и, что более важно, сформированных требований и ожидаемых результатов. Предлагаю использовать эту структуру семи А в случаях использования ИИ общественной безопасности:

Эта структура не представляет собой обязательный 7-этапный процесс, который должны использовать агентства общественной безопасности для реализации приложений ИИ, она не обязывает соблюдать приведенную последовательность. Однако она ранжирует сложность в реализации приложений ИИ от «анализа» до «автономности»:

1.Analyze Анализ: Самое основное и легко достижимое - от анализировать текстовые данные, фото, видео, аудио и даже данные от сенсоров. Такой анализ должен создавать текстовое преобразование, описание и пометки для анализируемого элемента данных.

2.Automate Автоматизация: Общественная безопасность включает в себя множество рутинных процедур, которые могут быть автоматизированы за счет применения ИИ. Примеры включают ежедневную генерацию отчетов о преступлениях, обучение сотрудников на основе ранее полученных навыков, классификацию фотографий места преступления, публикацию резюме фактов расследования и составление списка транспортных средств.

3.Assess Оценка: Это этап, где реализации ИИ начинает становиться интересной. Эта возможность выходит за рамки анализа элементов точечных данных и предполагает оценку общей картины. Вне знания того, что и когда, оценка должна решать, почему и как, например, почему ряд подобных преступлений был совершен по соседству или как человек радикализован для поддержки терроризма.

4.Augment Усиление: Хотя почти все работы по обеспечению общественной безопасности регулируются законами, многие решения должны приниматься сотрудниками полевых подразделений на основе их ситуационной оценки, знаний и опыта. Вот почему в некоторых отраслях ИИ чаще называют дополненным интеллектом. Это дополнение, а не замена человеческому интеллекту. Речь идет о помощи людям стать быстрее и умнее в задачах, которые они выполняют. Например, представление ежедневных областей, подверженных преступности, и присутствие прошлых преступников в этих областях соответствующим офицерам для принятия решения.

5.Assist Помощь: Уровень, где человек использует ИИ как помощника, желательно, общаясь на естественном языке. Используя тот же пример в разделе «Усиление», помощник может предложить офицеру маршрут патрулирования, места посещения и людей для проверки на основе приоритетов, срочных отправок и анализа затрат и результата.

6.Anticipate Предвидение: Использование приложений AI для прогнозирования, предположения таких явлений, как преступления, беспорядки, катастрофы, дорожно-транспортные происшествия и даже местонахождение подозреваемых.

7.Autonomize Автономность: Не совсем «Robocop», но система, включающая программное приложение, беспилотный летательный аппарат, автомобиль или робот, который работает автономно без или с малым вмешательством человека. Возможно, использующий оружие, но это уже предмет юридической и этической дискуссии.

Эта модель семи А служит основой для практических служб общественной безопасности, чтобы использовать при разработке своих приложений ИИ. Позвольте привести больше примеров здесь через отдельные функции общественной безопасности и концептуализировать возможности ИИ через семь А.

Патрулирование и защита границ: Анализ вторжения человека или транспортного средства; оценить вероятность попадания дикого животного; предвидеть точки контрабанды и в автоматическом режиме запускать БПЛА.

Опасные вещества: Автоматизированное отслеживание перемещения опасных веществ и усиление человека информацией о прохождении данного транспорта вблизи объектов критичной инфраструктуры или особо охраняемых территорий.

Эксплуатация детей: Анализ социальных медиа и оценка вероятности принуждения детей к противоправным действиям сексуального характера. Помощь человеку в обнаружении и предвидение дальнейших действий преступника.

Опасные инциденты: Анализ социальных медиа и видеоданных для оценки вероятности опасного инцидента. Предвидение развития ситуации для ее предотвращения.

Online Радикализация: Автоматизация выявления вербовщиков. Помощь человеку в виде online-общения с вербовщиками для идентификации.

Стихийные бедствия: Оценить разрушенные районы с большинством выживших; усилить человека информацией о доступном на маршруте транспорте и вероятности повторения бедствия.

Управление, контроль и коммуникации: Автоматизация планирования патрулей с целью предотвращения преступлений, помощь человеку в принятии входящих обращений и диспетчеризации.

Противодействие БПЛА: Анализ дронов на принадлеж-

ность преступникам; предвидение расположения оператора БПЛА и автономность контрудара по враждебному дрону.

Оповещение населения: Автоматизация тестирования системы и оценка рисков автономности в широковещательной рассылке оповещений.

Перемещение выживших: Помощь человеку в определении степени ущерба здоровью спасенных для дальнейшего направления на оказание помощи или перемещения для восстановления и предвидение потребностей в запасах воды, пищи и медикаментов.

Физическое и цифровое место преступления: Автоматизация архива доказательств, помощь человеку в идентификации нестандартных предметов, изъятых с места преступления.

Семь проблем ИИ в обеспечении общественной безопасности.

1.Сверх ожидания: Хотя это и не Robocop, от некоторых из приведенных выше примеров часто ожидают большего, чем реально можно получить, особенно это актуально для служб, создаваемых с нуля. Агентство или служба, должны начать с видения и дорожной карты реализации. Ставьте амбициознную цель, но начинайте с малых шагов, используя модель семи А для установки приоритетов этапов и определения желаемых результатов.

2.Внутреннее противостояние: Главная проблема - в боязни личного состава потерять рабочие места, службы должны пояснять, что данные нововведения являются поддержкой для получения более высоких результатов. Также очень важно вовлекать личный состав в процесс внедрения ИИ для использования наработанного опыта при формировании алгоритмов.

3.Общественное доверие: Боязнь неизвестного может привести к общественному недоверию. Открытость и регулярное взаимодействие с общественностью является ключевым, особенно при формировании доверия во время перехода к Объединенной общественной безопасности.

4.Конфиденциальность: Приложения ИИ не только анализируют большие данные, но и разрабатывают профиль и мнение о людях. Защита частной жизни является обязательным условием для поддержания общественного доверия с целью предотвращения дискриминации по какому-либо признаку.

5.Алгоритмические смещения: Уже есть случаи, когда системы ИИ учатся у человека и становятся расистскими, сексистскими и предвзятыми. Может потребоваться прозрачность и регулярный обзор алгоритмов.

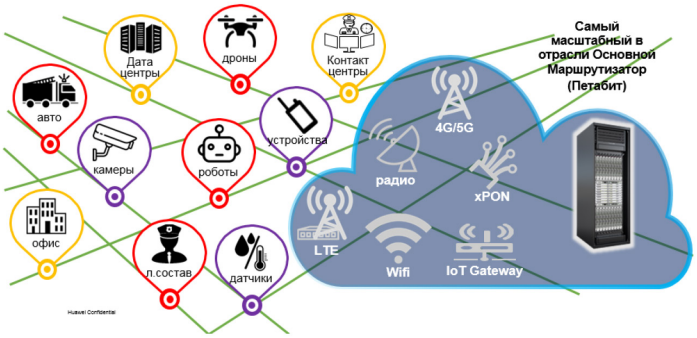
6.Законы и этика: Использование систем ИИ должно обязательно соответствовать законам. Более сложным является вопрос о том, является ли такое использование этичным, например автономное принятие решения о убийстве вооруженного преступника, создающего непосредственную опасность для других. Службе, возможно, потребуется подготовить набор этических руководящих принципов использования ИИ.

7.Реализация: Хотя ИИ - это больше, чем просто проект в области ИКТ, нам все еще необходимо рассмотреть вопросы технологической реализации, которые будут рассмотрены в следующем разделе.

Семь аспектов реализации

1.Связность

Часто это упускается из виду, но связность имеет решающее значение. Так же, как пять органов чувств человека собирают «данные» до того, как мозг принимает решение, системы искусственного интеллекта нуждаются во всех источниках данных для лучшей обработки. Связность, особенно беспроводная для обеспечения мобильности, критически важна.



Huawei имеет самый полный выбор технологий, как проводных так и беспроводных, для подключения к разнообразным источникам данных, а также крупнейший в отрасли петабитный маршрутизатор для управления огромным объемом данных

2.Big Data

ИИ может быть реализован с помощью жесткого кодирования на основе правил или машинного обучения, которое можно задать с помощью дерева решений, индуктивной логики или глубокого обучения. Общим знаменателем всех методов является требование большого объема, высокой скорости и большого разнообразия данных-Big Data:

Платформа больших данных FusionInsight компании Huawei предлагает обширный набор услуг, включая Hadoop, Spark, Flink и LibrA. Платформа даже имеет более двухсот собственных моделей данных и алгоритмов, специально разработанных для систем обеспечения общественной безопасности, что позволяет партнерам и клиентам быстро разрабатывать свои собственные приложения. Эта платформа подходит для четырех сценариев:

Вычисления не в режиме реального времени, связанные с большими данными и сниженными требованиями по задержке.

Вычисления в памяти с умеренными требованиями к низкой задержке.

Потоковые вычисления в реальном времени с более строгими требованиями по задержке.

Массивный анализ структурированных данных.

3.Вычислительная мощность

Большие данные требуют больших вычислительных мощностей. ИИ по существу управляется данными, результат должен быть точным и быстрым. Не все оборудование и системы создаются одинаково. Huawei использует специализированное оборудование для лучшей поддержки четырех сценариев, упомянутых ранее.

В дополнение к аппаратным инновациям Huawei, платформа FusionInsight big data может работать на облачных технологиях Huawei для лучшего объединения ресурсов (вычисления, хранения и сети).

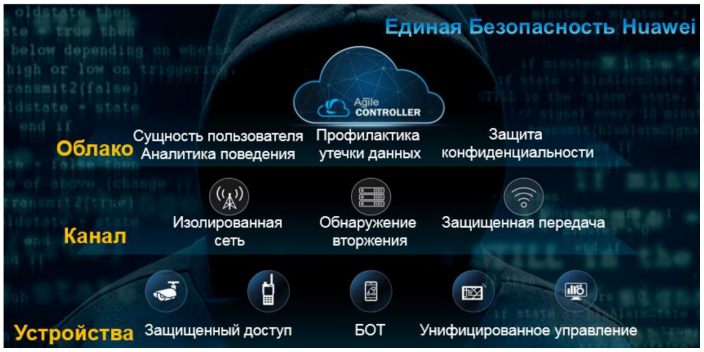
4.Применение платформ

В некотором смысле приложения ИИ ограничены воображением, и службы, обеспечивающие безопасность населения, могут использовать структуру 7 А для концептуализации и приоритезации таких приложений. Нужно, чтобы платформы облегчали быструю разработку приложений ИИ, не беспокоясь об аппаратной интеграции и производительности, не требуя поиска и подключения к источникам данных и даже наличия общих компонентов для использования без необходимости их кодирования в приложениях. Вот почему Huawei разработал набор платформ C-C4ISR для обеспечения объединенной общественной безопасности.

Эти платформы вместе с приложениями партнеров применимы не только для больших городов. Существуют десятки тысяч городов с населением менее миллиона человек. Безопасность этих населенных пунктов не менее важна, нужен доступ ко всем уровням данных, чтобы получить более точную информацию для эффективной работы ИИ. Именно поэтому Huawei предлагает компактные решения Safe City для таких средних городов. Safe City Compact также может использоваться в различных сценариях.

5.Кибербезопасность

Работая с огромным объемом данных, и в основном конфиденциальных, службы общественной безопасности должны принять дополнительные меры предосторожности для обеспечения своей кибер-безопасности. Любая утечка данных, безусловно, нарушает защиту конфиденциальности и снижает доверие общественности. Манипулирование данными может привести к нежелательным и даже неправильным результатам работы ИИ. Ниже приведена схема единого решения по безопасности от компании Huawei:



6.Непрерывные инновации

Внедрение ИИ - это долгий путь, и мы должны использовать инновации для достижения наилучших результатов. По данным Всемирной организации интеллектуальной собственности, Huawei стала лучшей компанией в 2017 году во всем мире и во всех отраслях промышленности, применив наибольшее количество патентов, 4024, если быть точным. Не так давно Huawei запустила два продукта, связанных с искусственным интеллектом: программно определяемую камеру и Intent-Driven Network (решение, позволяющее анализировать цели и намерения пользователей сети), которые являются частью устройств с применением ИИ и инфраструктуры ИИ, соответствуя четвертому технологическому уровню, упомянутому выше.

7.Отраслевая экосистема

ИИ не может быть внедрен силами только одной компании, необходима целая экосистема. Реализация должна следовать открытым стандартам, чтобы гарантировать отсутствие зависимости от поставщика решения. Huawei поддерживает и принимает более 30 открытых стандартов, ее партнерами уже являются более 1000 компаний, внедряющие собственные приложения. Эти партнеры пользуются мощностями наших открытых лабораторий OpenLab по всему миру.

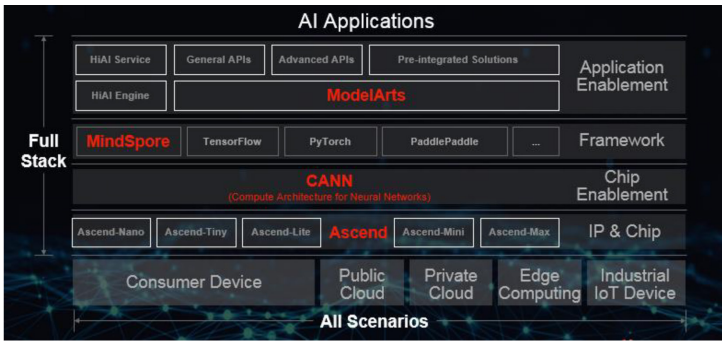
Как лидирующая на рынке ИКТ, компания Huawei предлагает полный набор решений с использованием ИИ, чтобы использовать максимальный диапазон технологий - от устройств до подключения к облачной платформе:

Серия Ascend специализированных чипов на основе единой масштабируемой архитектуры.

Библиотеки для САШ чипов и высокоавтоматизированный инструментарий для операционной разработки.

MindSpore - фреймворк обучения, набор («конструктор») для web-разработчиков приложений и сервисов при создании ИИ.

Использование приложений для сквозных сервисов (ModelArts), многоуровневых API и предварительно интегрированных решений, таких как решения для общественной безопасности.



Более 6000 специалистов вовлечены в работу по направлению обеспечения общественной безопасности компании Huawei, в том числе многие с опытом работы в службах и агентствах, обеспечивающих правопорядок, и это позволяет разрабатывать архитектуру для реализации ИИ: технологическую бизнес-архитектуру, архитектуру данных и архитектуру приложений.

Заключение

Цифровая трансформация общественной безопасности, Объединенная общественная безопасность не может ждать, мы рискуем столкнуться с развивающимися угрозами и операционными проблемами. Требования и ожидаемые результаты диктуют варианты использования ИИ. Уровни 7 А могут помочь определить и приоритезировать то, что нужно в ИИ: Анализ, Автоматизация, Оценка, Усиление, Помощь, Предвидение и Автономность.

Следует обратить внимание на варианты преодоления семи проблем: чрезмерное ожидание, внутреннее сопротивление, доверие общественности, конфиденциальность, алгоритмические предубеждения, законы, этика и проблемы реализации. Нужно фокусироваться на семь областей, когда речь заходит о фактической реализации ИКТ проектов ИИ: Связность, Big Data, Вычислительная мощность.

Василевский Сергей Владиславович,
генеральный директор ООО «Арсенал67»

Комплексный подход к созданию Единой системы розыска и поиска транспортных средств Российской Федерации в интересах силовых структур (ЕСРПТС РФ)

Создание ЕСРПТС является важнейшей государственной задачей, способной существенно влиять на эффективность раскрытия преступлений, розыска лиц, скрывающихся от следствия и суда, предотвращения незаконного оборота оружия и наркотиков, предотвращения террористических угроз, а также борьбы с контрабандой и ввозом санкционной продукции. В этой связи нами предлагается следующий комплекс мероприятий:

1. Использовать десятки тысяч ранее установленных комплексов фотовидеофиксации (ФВФ) для решения этой задачи.

2. Изменить подход МВД России в отношении требований к местам установки комплексов ФВФ. В настоящее время по требованию ГУОБДД МВД России комплексы должны устанавливаться в местах аварийности. Различные коммерческие и государственные структуры при установке новых комплексов выбирают места с наибольшим трафиком и возможностью получения большего количества штрафов для их самоокупаемости. Необходимо при размещении комплексов учитывать места оперативного интереса силовых структур и все возможные въезды-выезды с контролируемой территории. Так, в Смоленской области определенный процент комплексов ФВФ устанавливается именно в таких местах по протоколу между владельцем комплексов, УМВД и УФСБ по Смоленской области.

3. Изменить требования к владельцам комплексов ФВФ по получению данных с них. Необходимо получать весь поток проезжающих транспортных средств, а не только фото нарушений.

4. Изменить сроки хранения фото- и видеоматериалов, полученных с комплексов ФВФ. В настоящее время этот срок составляет в среднем по России от 1 до 3 месяцев и касается только нарушений, а не всего потока ТС.

Например, в Смоленске срок хранения фотоматериалов всего потока составляет 3 года, видеоматериалов - от 1 месяца до года в зависимости от оперативной необходимости.

5. Осуществлять мониторинг работы всех комплексов ФВФ, задействованных в ЕСРПТС, для контроля их работоспособности в онлайн- режиме. В случае выхода комплекса из строя силами подрядных организаций немедленно принимать меры к восстановлению его работоспособности.

6. В целях реализации пунктов 3,4,5 принять на снабжение или разработать новое программное обеспечение (ПО) в совокупности с аппаратными средствами, осуществляющими хранение информации с нижеперечисленными требованиями к системам АПК.

Система визуального отображения расположения фоторадарных комплексов в реальном времени - предназначена для координации работы, визуального отображения местоположения, обеспечения взаимодействия со смежными системами комплекса.

Система картографии свободно редактируемой детальной карты - предназначена для привязки фоторадарных комплексов к географическим объектам, идентификации местоположения фоторадарных комплексов, корректировки правильности разворачивания передвижных комплексов оператором системы в реальном времени.

Система получения информации о месторасположении передвижных фоторадарных комплексов.

Система розыска (государственных регистрационных знаков) транспортных средств, занесенных в базы розыска, в потоке получаемых от комплексов ФВФ и сведений о зафиксированных транспортных средствах в реальном времени.

Система поиска отдельных номеров , или части номеров, ГРЗ в базе зафиксированных транспортных средств.

Система одновременного отображения видеоизображения с нескольких фоторадарных комплексов.

Система отображения потока фотоматериалов о нарушениях ПДД, поступающих в режиме реального времени со всех подключенных фоторадарных комплексов.

Система получения видеоизображения в реальном времени с фоторадарных комплексов.

Система отображения списка зафиксированных транспортных средств.

Система статистики и анализа накопленной информации, с выводом графически развернутых схем и графиков.

Система поиска зафиксированных транспортных средств позволяет получать информацию о перемещениях ТС, зафиксированных системой, и строить пространственные маршруты движения с дальнейшим переносом данных в систему картографии. Комплектуется модулем нейронного поиска, который позволяет выводить приблизительное время и место следующего появления ТС.

Система, отображающая перемещения передвижных фоторадарных комплексов в режиме реального времени и фиксации расположения приборов на протяжении всего времени ее работы.

Система хранения полученной от фоторадарных комплексов информации с доступностью 24/7, резервированием, расширяемостью на «горячую» и начальным объемом, рассчитанным на 365 дней или более.

Система интеграции с мобильными устройствами, содержащими средства навигации.

Система первичной обработки нарушений ПДД.

Система синхронизации работы в реальном времени, распределения информационных потоков и нагрузки, получаемых с комплексов фотофиксации.

Система диагностики работы комплексов фотофиксации.

Система контроля, синхронизации и восстановления потерянных данных при передаче по нестабильным каналам связи.

Система администрирования.

Система защиты информации.

Возможно разработать и другие требования к ПО ЕСРПТС, кроме перечисленных.

Подобный АПК (АПК «РИФ») разработан компанией «Арсенал67» и применяется на протяжении четырех с лишним лет в Смоленской области в качестве ЕСРПТС в интересах УМВД, УФСБ по Смоленской области и ФТС России. Также в настоящее время АПК «РИФ» в тестовом режиме используется в Чеченской Республике, городе Санкт-Петербурге и Республике Беларусь.

Построение ЕСРПТС РФ должно происходить по **РАСПРЕДЕЛЕННОЙ** схеме, когда информация хранится на локальных серверах в регионах, а центральные сервера лишь запрашивают необходимую информацию в онлайн-режиме. Данная схема гораздо эффективнее и экономически менее дорогая, чем схема с **ЦЕНТРАЛИЗОВАННЫМ** сбором и хранением информации.

7. Изменить требования к новым комплексам ФВФ (при необходимости и новый ГОСТ). Все комплексы ФВФ, кроме контроля за ПДД, должны:

иметь возможность распознавания максимального количества ГРЗ, включая ГРЗ стран СНГ и Евросоюза;

осуществлять запись видео в режиме 7/24 и хранить данное видео на собственном сервере комплекса не менее 1 месяца;

иметь возможность подключения дополнительных камер для осуществления видеонаблюдения в месте установки комплекса не только на проезжей части, но и в местах оперативного интереса силовых структур (дорожные карманы, стоянки, объекты инфраструктуры и т.д.);

в составе ПО иметь модули для ведения баз розыска различных силовых структур в независимом режиме на самом комплексе;

в составе ПО иметь модули аналитики по требованиям силовых структур (например, контроль по таможенным декларациям и др.);

при возникновении соответствующего требования комплексы должны оборудоваться средствами защиты информации.

Подобный комплекс («Дозор-К») был разработан и сертифицирован (№67234-17 в Госреестре СИ) компанией и с 2017 года успешно применяется в Смоленской области (более 40 комплексов), в Брянской области (в интересах ФТС России на пунктах пропуска Новые Юрковичи и Красный Камень), в Республике Беларусь. За 3 месяца опытной эксплуатации с помощью этих комплексов ФТС России на пунктах пропуска в Смоленской и Брянской областях было задержано 245 ТС с санкционной продукцией.

7. Для эффективной работы ЕСРПТС предлагается также использовать другие (мобильные) средства сбора информации о ГРЗ ТС, такие как:

бортовые комплексы ГИБДД, например, «Кибер-Шериф» (обзор первого заместителя Министра внутренних дел Российской Федерации генерал-полковника полиции А.В. Горового за 2018 год);

средства, которые могут устанавливаться на общественном транспорте и рейсовых автобусах (например, «Кибер-мини»);

средства, специализированные для распознавания номеров и работы с базами розыска (например, «Арбалет»).

Хочется обратить внимание, что при реализации задачи построения ЕСРПТС важно выполнение всех условий в комплексе для обеспечения ее эффективности.

Терехов Валерий Игоревич,
доцент кафедры «Системы обработки информации и управления» МГТУ им. Н.Э. Баумана,
кандидат технических наук

Применение методов машинного обучения и нейронных сетей в задачах анализа неструктурированной информации и системах поддержки принятия решений

Неструктурированная информация (или данные) представляет собой информацию, либо не имеющую заранее определенной структуры данных, либо не организованную в установленном порядке. В большинстве случаев неструктурированные данные представлены в форме текста, который содержит такие сведения, как даты, цифры и факты. При этом, по многочисленным оценкам, более 70—80 % от всех данных в организациях - это неструктурированные данные.

Искусственный интеллект — это область информатики, занимающаяся разработкой интеллектуальных компьютерных систем, т.е. систем, обладающих возможностями человеческого разума - пониманием языка, обучением, способностью рассуждать, решать проблемы и т. д.

В свою очередь сильный искусственный интеллект – это программное обеспечение, благодаря которому компьютеры смогут думать так же, как и люди, а слабый искусственный интеллект – широкий диапазон технологий, которые могут добавляться в существующие системы и придавать им различные «разумные» свойства.

Рассмотрение приведенных в докладе подходов ведется с точки зрения слабого искусственного интеллекта.

И наконец, интеллектуальный анализ данных (Data mining) – это совокупность методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности

В символическом ИИ (типичным представителем которого являются экспертные системы) предметные эксперты вводят правила и данные для обработки в соответствии с этими правилами и получают ответы.

В отличие от символического искусственного интеллекта, в машинном обучении люди вводят данные и ответы, соответствующие этим данным, а на выходе получают правила, которые потом применяют к новым данным.

Глубокое обучение характеризуется как класс алгоритмов машинного обучения, который:

использует многослойную систему нелинейных фильтров для извлечения признаков с преобразованиями. Каждый последующий слой получает на входе выходные данные предыдущего слоя. Система глубокого обучения может сочетать алгоритмы обучения с учителем и без учителя, при этом анализ образца представляет собой обучение без учителя, а классификация — обучение с учителем;

обладает несколькими слоями выявления признаков или параметров представления данных (обучение без учителя). При этом признаки организованы иерархически, признаки более высокого уровня являются производными от признаков более низкого уровня;

формирует в процессе обучения слои на нескольких уровнях представлений, которые соответствуют различным уровням абстракции; слои образуют иерархию понятий.

На слайде в виде множеств приведены отношения между искусственным интеллектом, машинным и глубоким обучением.

Предлагаемый нами подход к созданию системы поддержки принятия решений по предотвращению угроз государственной и общественной безопасности основан на учете положений основополагающих правовых документов. Основные принципы соблюдения прав граждан и обеспечения их безопасности закреплены Конституцией РФ. Конкретные правовые нормы раскрываются в законах, указах Президента РФ, ежегодных Посланиях Президента РФ, других нормативных правовых актах.

Важнейшим документом является Стратегия национальной безопасности Российской Федерации.

Построение информационных систем мониторинга, анализа и прогнозирования угроз государственной и общественной безопасности основано на автоматическом извлечении слабоструктурированной информации из различных источников, включая потоки больших данных, машинном анализе текстов и подготовке предлагаемых решений на основании этого анализа. При этом активно применяются методы машинного обучения и нейронных сетей.

Общая структура решения задачи оценки возможных угроз государственной и общественной безопасности и формирования предложений по принимаемым решениям, реализующая метод анализа иерархий (МАИ), включает, в том числе, средства анализа исходной информации, которые пользователь-аналитик использует для обоснованного формирования экспертных оценок в методиках оценок угроз. Таких методик может быть много. Они могут использовать для выработки решений разный методологический аппарат, разные исходные данные, относиться к разным сферам угроз безопасности. Использование МАИ позволяет выработать общую оценку угрозы безопасности и подготовить проект рекомендаций, которые оптимальным образом обобщат рекомендации, получаемые частными методиками. Отдельные методики используют разные методы, в том числе машинное обучение, нейроалгоритмы и т.д.

Нами реализован ряд методик оценки обстановки и выработки предложений по предотвращению развития кризисных ситуаций, которые были предоставлены Военной академией Генерального штаба Вооруженных Сил Российской Федерации. Потребовались существенные доработки для того, чтобы обеспечить работу системы в автоматизированном и автоматическом режимах. В условиях ограниченного времени компьютерная система, работая в автоматическом режиме, может сама провести оценку обстановки и подготовить предложения, направленные на противодействие выявленным угрозам. При работе в автоматизированном режиме все формируемые системой оценки и предложения выда-

ются оператору, который может принять их или внести изменения, после чего формируется отчет и отображение результатов средствами геоинформационной системы.

Возможен многопользовательский режим, когда группы экспертов работают со своей исходной информацией с использованием определенных методик в единой информационной среде. Руководитель следит за ходом выполнения работы со своего рабочего места, может корректировать действия рабочих групп и принимает окончательное решение.

Логикой решения задачи оценки угроз государственной и общественной безопасности при функционировании предлагаемой Системы можно выделить четыре этапа обработки информации, которые определяются:

1. Сбор информации, который выполняется в автоматическом режиме;

2. Систематизация информации по различным факторам. Система позволяет осуществить настройку факторов и признаков систематизации информации.

3. Оценка вероятных угроз безопасности, которая проводится по различным методикам. Результатом оценки являются численные показатели, которые характеризуют выявленные угрозы по факторам, странам и направлениям.

4. Подготовка предложений. Формируется отчет, включающий выявленные угрозы и предложения по их нейтрализации.

На этапе сбора информации от различных источников при анализе потоков новостных сообщений проводится обнаружение и удаление дублирующих сообщений, определяются оригиналы сообщений, выявляются события и определяется их тематическая направленность, осуществляется геопривязка сообщений и событий, производится оценка достоверности сообщений. Все указанные операции выполняются автоматически, для управления этим процессом разработана специальная программа управления сбором информации. Для этого используется машинное обучение - машина опорных векторов (SVM). SVM - набор схожих алгоритмов обучения с учителем, использующихся для задач классификации и регрессионного анализа. Основная идея метода - перевод исходных векторов в пространство более высокой размерности и поиск разделяющей гиперплоскости с максимальным зазором в этом пространстве.

С октября 2015 года начат сбор информации с различных сайтов федеральных и региональных органов власти, основных новостных агентств, федеральных и региональных СМИ. Организован также сбор информации от ряда англоязычных источников, что позволяет проводить совместный компьютерный анализ информации на русском и английском языках, выявлять признаки информационных вбросов и уточнять оценки достоверности сообщений, поступающих от различных источников. Имеется техническая возможность осуществлять сбор и анализ информации на других иностранных языках.

Нами проработана методика мониторинга и прогнозирования развития угроз безопасности, основанная на принципах анализа потоков текстовых сообщений, которую условно можно назвать «4С+П». Она предполагает выполнение анализа потока текстовых сообщений, загружаемых с веб-сайтов или из специализированных источников. В этом потоке выявляются события, относящиеся к угрозам национальной безопасности. На основе обнаруженных событий выполняется отслеживание развития ситуаций и определение возможных сценариев их дальнейшего развития, а также подготовка предложений.

Для ситуационного прогноза применяется метод исторической аналогии. Идея метода состоит в обнаружении для текущей ситуации аналогичных ей эталонных ситуаций. При этом предполагается, что обнаруженные аналоги представляют собой возможные сценарии дальнейшего развития текущей ситуации.

С целью последующего формирования предложений, при подготовке эталонных ситуаций эксперты должны снабжать их рекомендациями, каждая из которых предписывает, какое лицо, какие действия и в какой срок должно выполнить.

Предполагается выделение наиболее вероятного, оптимистичного и пессимистичного сценариев. Наиболее вероятный сценарий формируется на основе эталонной ситуации, наиболее близкой к текущей. Для выделения наиболее оптимистичного и пессимистичного сценариев выполняется определение приоритетов сценариев с помощью метода анализа иерархий.

Структура системы обработки потоков больших данных показывает как с ее помощью можно осуществлять обработку и глубокий анализ потоков разнородных данных, поступающих от различных датчиков, систем видеонаблюдения и других источников. На основе собранных и агрегированных данных строится обогащенная семантическая модель, которая используется для мониторинга и прогнозирования развития ситуаций с целью поддержки принятия управленческих решений. Использование методов машинного обучения обеспечивает возможность гибкой настройки в соответствии с потребностями пользователей. Для достижения высокой эффективности использования полученных результатов анализа потока данных лицом, принимающим решения, применяются методы когнитивной компьютерной графики. Рассмотрим модельный пример использования обработки потоков больших данных для обнаружения нештатных ситуаций на важных объектах обороны с использованием нейросетевых методов. Применяются две разные нейросети: сверточная сеть с глубоким обучением используется для анализа наблюдаемой сцены и выявления признаков нештатной ситуации, более простая нейронная сеть Хемминга - для уточнения ее признаков и наличия угрозы защищаемому объекту. В данном примере показана возможность определения элементов спецодежды и наличия оружия у нарушителя.

Рис. 1

На рис. 1 представлены элементы многоагентной системы, решающей задачи обеспечения безопасности, которая состоит из разнородных нейроагентов.

На рис. 2 показано применение методики для анализа угроз государственной и общественной безопасности, связанной с деятельностью несистемной оппозиции в период начала подготовки к предвыборной президентской компании 2018 года. Слева - результаты анализа сообщений о митингах и протестах, которые имели место в ходе предыдущих выборов. На правом рисунке

Анализ угроз государственной и общественной безопасности

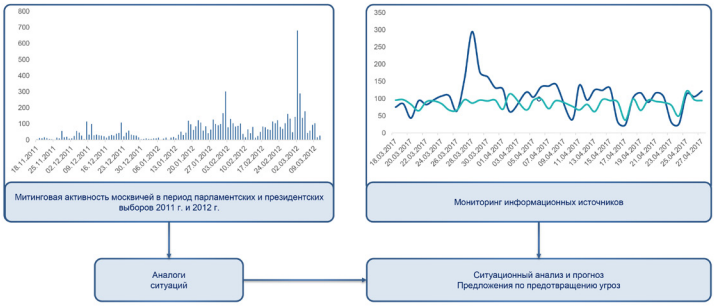


Рис. 2

показаны результаты анализа и прогноза развития протестной активности в 2017 году. Сопоставление текущей ситуации с имеющимися в прошлом аналогами позволяет применить метод исторической аналогии для определения возможных сценариев развития обстановки и выработки предложений по нейтрализации угроз.

Результаты выявления событий и ситуаций на примере митинга 12.06.2017

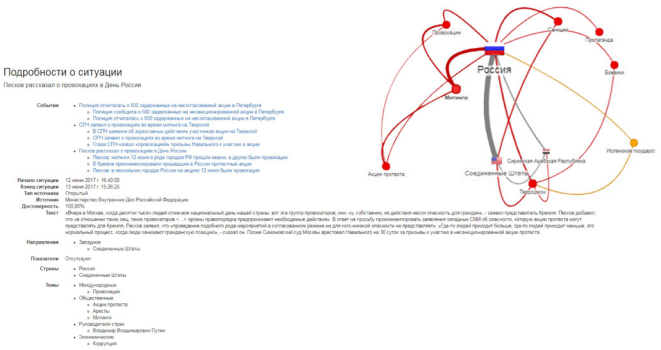


Рис. 3

На рис. 3 показаны результаты автоматического выделения событий и ситуаций на примере анализа сообщений о проведении несистемной оппозицией митинга 12.06.2017. Выделяются угрозы государственной и общественной безопасности, которые могут быть представлены в текстовом и графическом виде.

Для отображения результатов анализа в системе активно используются средства когнитивной компьютерной графики, и в частности метод анаморфирования.

Когнитивная компьютерная графика представляет собой методы визуализации данных, позволяющие активировать наглядно-образные механизмы мышления лица, принимающего решение, и облегчающие принятие решения в сложной обстановке или нахождение решения сложной проблемы.

Пример комплексного анализа информации. Преступления, связанные с незаконным оборотом оружия

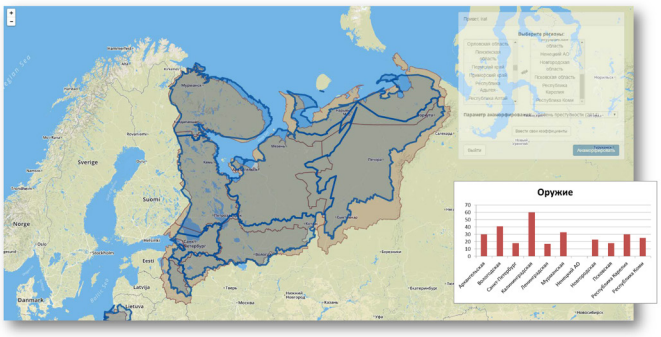


Рис. 4

Один из алгоритмов анаморфирования нами успешно реализован. Результаты показаны на рис. 4 на примере анализа статистики о преступлениях, связанных с незаконным оборотом оружия в СЗФО, и отображения их на карте.

Был создан удобный инструмент визуализации как первичных данных, так и большого объема собираемой и анализируемой актуальной геополитической информации. С его помощью стало возможным провести компьютерное моделирование изменений геополитических границ, что позволяет выявить и наглядно представить для лиц, отвечающих за выработку решений в области стратегии развития государства, потенциал и направления угроз безопасности России.

Пример комплексного анализа информации. Продолжение. Убийства и покушения на убийство

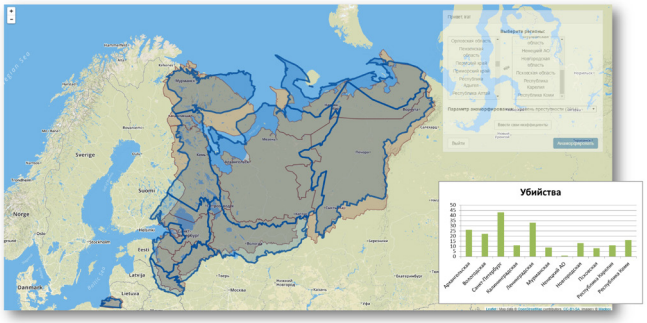


Рис. 5

На рис. 5 приведены результаты работы алгоритма анаморфирования для комплексного анализа статистики о преступлениях, связанных убийствами и покушениями на убийства в СЗФО, и отображение их на карте.

Рекомендации по предотвращению угроз государственной и общественной безопасности

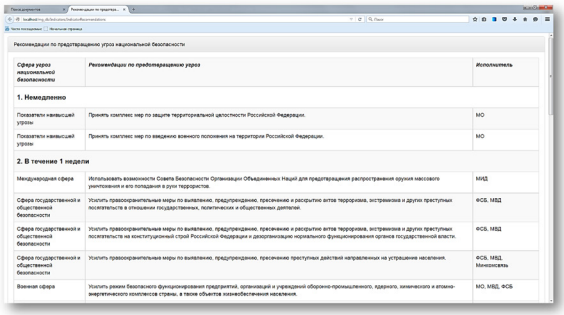


Рис. 6

На рис. 6 показаны результаты работы системы, связанные с подготовкой итогового отчета и предложений по ликвидации выявленных угроз государственной и общественной безопасности. Результаты могут отображаться на 2-мерной или 3-мерной карте, а также распечатаны в виде документа, который может включать в себя текстовую и графическую информацию.

Предлагаемая нами модель развития кризисной ситуации, методы прогнозирования обстановки и анализа потоков больших данных требуют значительных вычислительных затрат. Поэтому в МГТУ им. Н.Э. Баумана ведутся работы по созданию аппаратных средств, которые обеспечат существенное ускорение вычислений. Нами разработан принципиально новый процессор для обработки множеств, структур данных и графов. Процессор получил название Leonhard в честь Леонарда Эйлера. При низкой тактовой частоте его производительность сравнима с производительностью микропроцессоров семейства Intel Pentium, он имеет целый ряд других преимуществ по сравнению с иностранными аналогами.

Это достигается за счет параллелизма при обработке сложных моделей данных.

В рамках проекта «ТРОПОСФЕРА» разработан линейный ряд современных систем хранилищ данных нашей торговой марки «Baum». Реализованная архитектура обеспечивает практически безграничное масштабирование (до сотен узлов и сотен петабайт), простоту использования, независимо от объема, линейную масштабируемость и емкость, производительность, высокую эффективность и надежность. Она идеально подходит для решения задач, требующих хранения больших объемов данных.

Предлагаемый нами подход и разрабатываемый для его реализации в МГТУ им. Н.Э. Баумана программно-технический комплекс позволяет реализовать систему межведомственного информационного взаимодействия. Появляется возможность оценить значимость критериев и свести воедино выводы отдельных методик, получить некий инструмент сквозной межведомственной аналитики и детализации в области угроз безопасности. При этом выявленные угрозы отображаются в геоинформационной системе.

С помощью технологий, которыми владеют специалисты МГТУ им. Н.Э. Баумана для создания сложных информационных систем поддержки принятия решений в области обеспечения государственной и общественной безопасности, возможно создание самого современного программного обеспечения, отвечающего всем требованиям, включая требования защиты информации.

В МГТУ им. Н.Э. Баумана разработано программное обеспечение программно-технического комплекса по предотвращению угроз государственной и общественной безопасности, которое может функционировать под различными программными платформами (Windows, различные диалекты Linux, в т.ч. «Astra Linux Special Edition»).

При создании интерфейсных компонентов программ применяются средства веб-разработки, обеспечивающие функционирование на различных программно-аппаратных платформах (стационарные устройства, планшеты, смартфоны и т.д.).

Предлагаемая реализация программно-технического комплекса по предотвращению угроз государственной и общественной безопасности обеспечивает объединение результатов выполнения отдельных методик, в том числе методик различных ведомств, в единый программно-технический комплекс, все компоненты которого являются отечественными разработками и сертифицированы.

Для реализации методов машинного обучения и нейронных сетей в задачах анализа неструктурированной информации и системах поддержки принятия решений используется комплекс программ оценки военно–политической обстановки, предназначенный для формирования исходной модели военно-политической (стратегической) обстановки, выявления и оценки вероятных угроз национальной безопасности РФ, шифр «Выпускник-ВАГШ», выполненной в МГТУ им. Баумана в 2017 году, сертификат Минобороны России № 3767 от 20.11.2017.

Прудников Андрей Сергеевич,
генеральный директор ООО «Байтерг»
Ерошин Евгений Валерьевич,
директор по маркетингу ООО «Байтерг»

Персональные видеорегистраторы как часть экипировки «Цифрового полицейского»

Персональные видеорегистраторы (далее - ПВР) сейчас становятся все более популярными в полиции разных стран мира.

Пионерами в этой области являются США и Великобритания, а сейчас ПВР применяются уже в полиции Германии, Австралии, Гонконга, ЮАР, Бразилии, Индии и многих других стран на всех континентах.

Основываясь на мировом и российском опыте, можно заявить, что применение ПВР имеет следующие положительные эффекты:

1. Повышается дисциплина полицейских
2. Снижается количество случаев коррупции и взяточничества
3. Снижается количество спорных ситуаций
4. Снижается количество жалоб на полицейских
5. Уменьшается количество «бумажной работы» полицейских
6. Освобождается время для работы полицейских по защите правопорядка
7. Косвенный результат – повышается психологическая устойчивость и уверенность полицейских в своих действиях в опасных ситуациях
8. В целом повышается эффективность работы полицейских
9. Сбор доказательств в случаях правонарушений становится быстрее
10. Снижается количество случаев оскорблений и нападений на полицейских

Технологии и свойства персональных видеорегистраторов и их примеры реализации компанией «Байтэрг» в регистраторах марки «ДОЗОР»

1. Видеозапись

Качество видеозаписи – одна из ключевых характеристик персональных видеорегистраторов. Имеются модели с качеством SD/HD/FHD/SFHD.

В регистраторах «ДОЗОР-77» реализовано качество FHD - Super-HD 1296p, которое позволяет фиксировать лица людей на дистанции до 12 м.

2. Аудиозапись

Для аудиозаписи должен использоваться встроенный влагозащищенный микрофон, позволяющий фиксировать человеческую речь на дистанции 3-5 м. Именно такой используется в регистраторах марки «ДОЗОР».

3. Ночной режим

Полицейские работают днем и ночью, поэтому ПВР должен обеспечивать круглосуточную видеозапись с ночным режимом и подсветкой.

В регистраторах «ДОЗОР» реализован ночной режим с автоматической ИК- подсветкой с возможностью ручного управления.

4. Батарея

Продолжительности автономной работы должно хватать на смену полицейского.

В регистраторах «ДОЗОР-77» батарея обеспечивает 9-часовую автономную видеозапись.

В новом поколении «ДОЗОР-77 -01» будет реализована 14-часовая запись.

Запись продолжительностью 24 часа может быть реализована с подключением внешнего аккумулятора.

5. Защита данных

Все записи ПВР должны быть защищены от несанкционированного доступа и редактирования как полицейским, так и злоумышленниками в случаях хищения или потери ПВР. В регистраторах «ДОЗОР» используется несъемное ПЗУ, доступ к которому возможен только с помощью специализированного ПО и пароля.

6. Исполнение корпуса

Существует 2 основных типа корпусов: «моноблок» и корпус с вынесенной видеокамерой. Наиболее эффективным представляется исполнение «моноблок», так как вынесенная видеокамера имеет кабель, который тянется вдоль тела полицейского и может мешать ему в работе.

Размеры и вес ПВР должны быть минимальны, чтобы не затруднять работу полицейского.

Размер «Дозор-77» - менее пачки сигарет, а вес - всего 100 г.

Регистратор должен быть всепогодным, защищенным от дождя и снега.

«Дозор-77» имеет класс защиты IP-65. Готов к работе в режиме 24*7*365.

7. Работа с записями

Для работы с записями требуются специальное ПО и терминалы подзарядки регистраторов, копирования и хранения данных.

Для «ДОЗОР-77» разработано несколько терминалов: «Терминал-28» - напольного исполнения, для подключения (функции скачивания записи и подзарядки) 28 регистраторов, с сенсорным экраном, защищенным отсеком для установки регистраторов, встроенной видеокамерой фиксации действий оператора и дисковым массивом на месяц хранения записей с 28 регистраторов. При посменной работе обеспечивается подключение 56 ПВР; «Терминал-6» - настольного исполнения, для подключения (для скачивания записи и подзарядки) 6 регистраторов, с дисковым массивом на 2 недели хранения записей с 6 регистраторов. При посменной работе обеспечивается подключение 12 ПВР; «Нанотерминал» - устройство для копирования записей с регистратора «ДОЗОР-77» непосредственно на «флешку» и подзарядки регистратора.

8. Позиционирование

Встроенные модули позиционирования позволяют при просмотре записей видеть позицию и маршрут полицейского на карте.

В «ДОЗОР-77 new» реализован модуль позиционирования ГЛОНАСС.

9. Передача данных

Современные беспроводные технологии позволяют в реальном времени передавать видеопоток с ПВР по сетям 3/4G, WiFI.

Сейчас данная функция реализована в новой модели «ДОЗОР-4G+». Кроме того, «ДОЗОР-4G+» обеспечивает двустороннюю аудиосвязь, возможность передать тревожный сигнал и просмотр видео с него одновременно с позицией сотрудника на карте.

Видеоданные с «ДОЗОР-4G+» могут быть по сети объединены с видеоданными со стационарных и автомобильных систем видеонаблюдения для построения централизованных многоканальных систем.

Минатулаев Шахсолтан Магомедрасулович,
главный конструктор АС «ПЭК» ОАО «НПО Ангстрем»

Нынешнее применение и перспективы развития автоматизированной системы «Персональная электронная карта»

Группа компаний «Ангстрем» - современный высокотехнологичный холдинг, объединяющий в себе разработку и производство автоматизированных систем, новейших полупроводниковых приборов и телекоммуникационной аппаратуры.

Обладает двумя заводами по производству микросхем и предприятием по производству высокотехнологического оборудования и самых современных государственных автоматизированных систем по профилю особо защищенных в условиях цифровизации, включая специальные программы Минобороны России. Все средства приняты на снабжение приказом Министра обороны России.

В Минобороны России впервые создана и принята на снабжение (приказ Министра обороны России от 13.07.2017 № 439) автоматизированная система учета персональных данных военнослужащих, призывников и гражданского персонала, основанная на современных информационных технологиях отечественного производства, для создания единого информационного пространства.

Основными элементами системы являются персональная электронная карта (ПЭК) и жетон (ЭЖВ), позволяющие хранить более 300 параметров, включая биометрические характеристики, и применять персональную электронную подпись.

Карта военнослужащего нового поколения

Карта военнослужащего нового поколения завершает сертификацию в 8 Центре ФСБ России по профильным проверкам на перспективу использования как современная система защиты информации.

Сертификация проводится на протяжении более 3-х лет. Это связано с тем, что необходимо выработать самые передовые средства защиты информации. Российским экспертным организациям важно было также разработать особые требования к современным средствам защиты информации.

Важно понимать, что современный мир изменчив и потенциальный противник прогрессирует в плане использования средств воздействия на российские системы защиты информации.

Особо стоит отметить, что криптозащищенные средства и носители информации являются прямыми защитниками интересов государства в условиях высокотехнологического общества и развития технических средств, которые могут создать условия к подделыванию документов учета.

Карта нового поколения – отечественная, так как разработана и может производиться на единственном современном предприятии-производителе микропроцессоров в России АО «Ангстрем-Т».

Состав по типу средств оснащения АС «Паспорт» и их функциональности

Существует 5 основных видов и 11 типов оснащения объектов автоматизации. К основным видам относятся:

военкоматы субъектов Российской Федерации (подвид – военкоматы муниципальные, специальные войсковые части);

войсковые части (ряд типов оснащения в зависимости от функциональных требований);

медицинские учреждения. Данный вид оснащения является адаптивным к конкретному месту автоматизации, предприятие делегирует выработку требований к функциональному заказчику, имеют новые типы оснащения – госпиталь, поликлиника, часть, боевой расчет или передовой;

образовательные учреждения. Данный вид оснащения является адаптивным к конкретному месту автоматизации, предприятие делегирует выработку требований к функциональному заказчику, имеют новые типы оснащения – ВУЗ, колледж, специальные образовательные учреждения;

специальные и особые организации.

Преимущества использования в войсковых частях АС «Паспорт»

Особо отмечу, что активно развивается. Она стала по сути прототипом всех известных систем, например УЛГ (удостоверения личности гражданина). Будем считать – гражданина Российской Федерации.

Система уже интегрирована во многие сторонние системы, включая СКУД и ряд специальных информационных систем Минобороны России. Это связано с прохождением службы, кадровым учетом, материально-техническим учетом, довольствием, аттестатом на вооружение и т.д.

Принимается программа развития до 2024 года. Все заинтересованные органы военного управления выдвигают свои актуальные требования к модернизации и развитию АС «Паспорт».

Прохождение службы на изделии 83т645

Как ранее указано, АС «Паспорт» уже интегрирована с рядом специализированных систем. Потенциал развития и интеграции Системы далеко не исчерпан.

Сегодня видны направления взаимодействия Системы, ряд которых уже реализован в той или иной мере, но может быть расширен:

доступ к данным ведомственных информационных систем;

контроль работы СКУД и перемещения военнослужащих, включая разрешения по перемещению, что имеет большое значение для важных объектов, включая особо охраняемые зоны;

контроль фактического получения продовольственного и вещевого довольствия, включая столовые и склады;

проверка путевых листов и сопровождающих лиц ,включая их предписания, через мобильные терминалы;

проверка военнослужащих ППС вне воинской части через мобильные терминалы.

Технические средства АС «Паспорт»

Специализированные устройства регистрации биометрических данных

Комплексы идентификации и биометрической регистрации осуществляют регистрацию биометрических данных (БД) на стационарных и мобильных пунктах контроля и регистрации, а также в машинах патрульно-постовой службы. Они предназначены для идентификации и верификации личности по биометрическим данным, а также для оформления и выдачи персональных электронных удостоверений сотрудникам полиции.

Стационарный комплекс регистрации БД (СКРБД)

Используется для проведения мероприятий по снятию биометрических характеристик человека с целью создания внутренней базы биометрических данных с возможностью последующего выпуска персональных электронных документов. Представляет собой готовое решение для установки в центрах регистрации биометрических данных. Дает возможность произвести регистрацию набора биометрических признаков человека (отпечатки пальцев рук, отпечатки ладоней, 2D-цифровое изображение лица). Дополнительно может оснащаться сканером радужной оболочки глаз.

Области применения биометрических характеристик – идентификация и верификация личности гражданина, сотрудников МВД России, мигрантов, лиц, находящихся под следствием, и заключенных, физических лиц, находящихся в беспомощном или бессознательном состоянии (переносное исполнение), контроль доступа в охраняемые здания и помещения, контроль доступа к защищаемым информационным системам.

Универсальный переносной комплекс регистрации БД (УПК)

Используется для выездного снятия биометрических данных в удаленных и труднодоступных местах с целью создания внутренней базы биометрических данных сотрудников с возможностью последующего выпуска персональных электронных документов. Дает возможность произвести регистрацию набора биометрических признаков человека (отпечатки пальцев рук, отпечатки ладоней, 2D-цифровое изображение лица). Дополнительно может оснащаться сканером радужной оболочки глаз. На данный момент УПК серийно поставляется в Минобороны России. Универсальное рабочее место идентификации – проведение опознания и подтверждения личности по биометрических характеристикам и персональным электронным картам.

Мобильное АРМ «Патруль»

Портативное малогабаритное устройство для идентификации и верификации личности субъекта в нестационарных условиях. Универсальное рабочее место патрульно-постовой службы с возможностью чтения персонального электронного удостоверения сотрудника МВД России, проведения биометрической проверки, фото-, видео- и аудиофиксации, регистрации текстовой информации.

Место установки – мобильные пункты контроля, патрульно-постовая служба.

Основные функциональные возможности:

ведение локального реестра фактов проверок патрульной службой комендатуры и результатов этих проверок непосредственно в комендатуре;

автоматическая загрузка результатов проверок из МАРМ «Патруль» в локальный реестр;

автоматическая выгрузка данных из локального реестра в Подсистему «Аналитика»;

идентификация и верификация владельцев ПЭК/ЭЖВ по биометрическим и идентификационным характеристикам;

формирование отчётов о результатах проверок;

ввод и отображение текстовой информации посредством сенсорного экрана;

определение координат изделия во время проверки.

Комплектность КПТС «Патруль» изделия (83т645, исполнение 2)

Функции изделия:

аутентификация оператора Н-23КР и радиостанций

поддержка до 5 независимых схем связи уровня бригады

хранение схем связи в зашифрованном и имитозащищенном виде

размер ключей – 512 бит

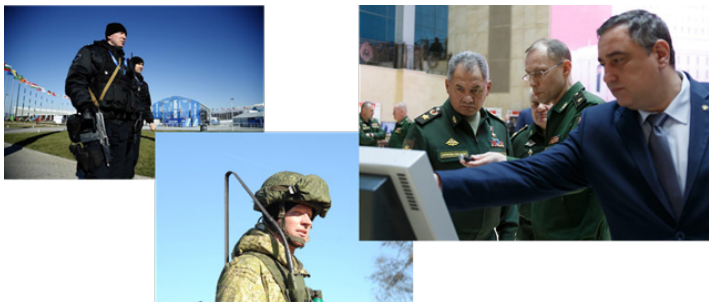
алгоритмы шифрования по требованиям ФСБ России

периодическая модификация ключей
наличие средств защиты от НСД
соответствие требованиям к криптографическим средствам по классу КА1
автоматическое стирание данных по истечении срока действия ключей
ведение журнала событий поддерживается в СПО-ОИ и ПАК-КР

Примеры использования при обеспечении безопасности граждан

XXII зимние Олимпийские игры и XI зимние Параолимпийские игры (Сочи, 2014 год)

Принято на снабжение и поставляется в войска с 2015 года



Персональное электронное удостоверение сотрудника МВД России (предложение)

Персональное электронное удостоверение (ПЭУ) сотрудника МВД России является персональным электронным документом, в который занесены в электронном виде и защищены средствами криптографической защиты данные: биометрические, медицинские, кадрового учета сотрудников и персонала.

Базовые идентификационные данные: фамилия, имя, отчество, дата рождения, личный номер, персональная фотография и т.д. представлены на карте, в том числе в графической форме, и размещены на лицевой стороне ПЭУ.

Персональное электронное удостоверение сотрудника также применяется как средство для вычисления и проверки квалифицированной электронной подписи и как электронный документ СКУД при получении доступа на объекты МВД России.

Сферы применения ПЭУ сотрудника МВД России:

электронное удостоверение личности сотрудника;

доступ к информационным ресурсам МВД России;

контроль прохождения контрольно-пропускных пунктов;

контроль доступа и нахождения на объектах, в том числе и защищаемых.

хранение и контроль персональных медицинских данных, заключений медицинских комиссий, результатов обследований и медицинских вмешательств;

хранение учетных данных при поступлении в учебное заведение МВД России, актуализация данных в ходе обучения, контроль нахождения в учебных аудиториях и на учебных объектах;

контроль получения продовольственного и вещевого имущества, иных видов довольствия.

Использование электронных жетонов военнослужащих

Во время Великой Отечественной войны идентификация военнослужащих осуществлялась по медальонам, сохранность которых не обеспечивалась в условиях высоких температур, а записи на бумаге - длительного времени хранения

В послевоенные годы введены личные жетоны военнослужащих из легких сплавов, которые используются и до настоящего времени. Обеспечивается их сохранность в условиях высоких температур и длительного времени, однако на них содержится только минимальная информация о военнослужащем (личный номер).

В рамках изделия 83т645 предусмотрено использование электронных жетонов военнослужащих
Встроенный микроконтроллер емкостью 160 кбайт обеспечивает хранение около 300 параметров.
Материал: износостойкий поликарбонат, втулка из медицинской стали с нанесенным личным номером.
Температура эксплуатации от -60 до +120˚С
Температура начала деформации поликарбоната +180˚С
Температура плавления стали более +1500˚С

Лукашев Николай Васильевич, подполковник полиции,
ведущий научный сотрудник отдела по исследованию стратегических проблем управления научно-исследовательского центра Академии управления МВД России ,кандидат физико-математических наук, доцент

Актуальные правовые и организационное проблемы внедрения современных информационных технологий в деятельность органов внутренних дел Российской Федерации

Деятельность органов внутренних дел Российской Федерации (ОВД) происходит в современных условиях доминирующей роли информации в основных сферах человеческой деятельности. В соответствии с основным положением Окинавской хартии информационного общества, которое было ратифицировано Российской Федерацией, «информационно-коммуникационные технологии (ИКТ) являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИКТ быстро становятся жизненно важным стимулом развития мировой экономики»[1]. Одновременно ст. 11 Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы гласит, что «информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка»[2].

Широкомасштабное внедрение ИКТ является следствием не только и не столько их физического появления в результате разработки и производства, сколько необходимости обеспечения обработки непрерывно возрастающего объема социальной и технической информации. Это явление, в частности, вызвало усложнение правовой системы в современном обществе, что может представлять угрозу существованию России как правового государства[3]. Например, сегодня в федеральном законодательстве насчитывается двадцать кодексов, в то время как в 1980 году их было всего девять. Одновременно возрастает объем нормативных правых актов. Так, Уголовный кодекс[4] РСФСР до 1994 года содержал 12 глав, в то время как современный УК состоит уже из 34 глав. Усложняется механизм правоприменения, в том числе в сфере управления деятельностью органов внутренних дел, что приводит к возрастанию информационной нагрузки как на исполнителей, так и на лиц, принимающих решения.

Так, среднее количество приказов, рассматриваемых и подписываемых министрами внутренних дел России после распада СССР, возросло более чем в четыре раза (см. рис.). При этом система управления в целом не претерпела существенных изменений.

Усложняется организационная структура и система управления ОВД. Количество взаимодействующих подразделений за последние десятилетия увеличилось приблизительно в 2-3 раза и составляет на муниципальном уровне управления порядка 30, на региональном – 60, федеральном - 120.

Среднее количество приказов, рассматриваемых и подписываемых министрами внутренних дел Россиискоя Федерации после распада СССР.

В условиях сохранения принципов единоначалия это существенно повышает требования к уровню компетентности и соответствующим личным качествам руководителей, в том числе к способности обрабатывать большой объём управленческой и правовой информации, вырабатывать оптимальные управленческие решения в ограниченных временных рамках.

Существенное усложнение механизма правоприменения, возрастание объёма и сложности процессуальной информации, высокая динамика социальных процессов являются причинами критического возрастания информационной нагрузки также и на исполнителей, в т.ч. дознавателей, следователей, оперативных работников в системе ОВД.

Таким образом, для обеспечения оперативно-служебной деятельности и эффективного управления ОВД необходимо привести организационно-штатную структуру, систему управления и информационного обеспечения в соответствие с современными требованиями.

Очевидно, что решить данную задачу при помощи одних лишь ИКТ невозможно. Необходим комплексный подход, основные принципы которого должны быть отра-

[1] Окинавская хартия глобального информационного общества. Принята 22.07.2000 лидерами стран «Большой Восьмёрки» // Дипломатический вестник. 2000. №8. С. 51–56.

[2] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Собрание законодательства РФ, 15.05.2017, № 20, ст. 2901.

[3] Лукашов Н.В. Усложнение правовой системы современного информационного общества, как угроза правовому государству // Труды Академии управления МВД России. 2012. № 3. С. 3–7.

[4] Далее – УК.

жены в концепции информатизации МВД России. Между тем в новейшей истории органов внутренних дел Российской Федерации данный подход нашел отражение лишь в приказе МВД России от 12 мая 1993 г. № 229 «О мерах по реализации концепции развития информационного обеспечения органов внутренних дел». Целью концепции провозглашалось «Совершенствование информационного обеспечения органов внутренних дел в борьбе с преступностью», при этом предусматривался комплекс мер по организационно-штатному обеспечению и обучению личного состава. Со временем цели принимаемых концепций информатизации сужались, всё более отдаляясь от проблем комплексного обеспечения оперативно-служебной деятельности и управления ОВД. Так, приказом МВД России от 30 марта 2012 г. № 205 «Об утверждении концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012 - 2014 годах» утверждена очередная Концепция, целью определено абстрактное «повышение уровня информационно-аналитического обеспечения деятельности МВД России».

Данная формулировка лишь фрагментарно способствует решению основных задач МВД России[5] :

1) выработка и реализация государственной политики в сфере внутренних дел;

2) нормативно-правовое регулирование в сфере внутренних дел;

3) обеспечение федерального государственного контроля (надзора) в сфере внутренних дел;

4) обеспечение защиты жизни, здоровья, прав и свобод граждан Российской Федерации, иностранных граждан, лиц без гражданства, противодействие преступности, охрана общественного порядка и собственности, обеспечение общественной безопасности, предоставление государственных услуг в сфере внутренних дел;

5) управление органами внутренних дел Российской Федерации;

6) обеспечение социальной и правовой защиты сотрудников органов внутренних дел, федеральных государственных гражданских служащих и работников системы МВД России, граждан, уволенных со службы в органах внутренних дел с правом на пенсию, членов их семей, а также иных лиц, соответствующее обеспечение которых на основании законодательства Российской Федерации возложено на МВД России.

Выводы

Для обеспечения эффективности оперативно-служебной деятельности и управления в системе МВД России необходимо скорректировать направления правового и организационного обеспечения внедрения ИКТ.

Предлагается концепцию собственно информатизации как процесса внедрения и использования информационных технологий дополнить (или разработать отдельную концепцию) в соответствии со следующими основными положениями:

приведение цели и задач информатизации в соответствие с целями и задачами деятельности МВД России, повышение правового статуса концепции информатизации;

развитие правовых основ использования информационных технологий в повседневной деятельности и для поддержки принятия решений;

повышение статуса и уровня ответственности IT-специалистов;

внедрение в повседневную практику технологий поддержки принятия решений и оперативного управления на основе ситуационных центров;

перераспределение штатной численности в пользу IT–специалистов при условии пропорционального повышения производительности труда сотрудников ОВД на основе IT и иных современных технологий.

Необходимо обеспечить соблюдение известных принципов информатизации, в противном случае затраты на приобретение дорогостоящих технологических решений будут недостаточно эффективными для решения актуальных проблем управления и оперативно-служебной деятельности ОВД в современных условиях.

Более подробное обсуждение проблемы и требует диалога с участием не только учёных и специалистов, но и лиц, принимающих решения в системе МВД России.

[5] Указ Президента РФ от 21.12.2016 № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации»

Кубасов Игорь Анатольевич,
полковник внутренней службы,
начальник Вычислительного центра
ФКУ «ГИАЦ МВД России»,
доктор технических наук, профессор

Перспективы развития интегрированных банков данных коллективного пользования регионального и федерального уровней. Организация эксплуатации и сопровождения ИБД-Р и ИБД-Ф

Предлагается рассмотреть вопросы организации эксплуатации и сопровождения программно-технических комплексов интегрированных банков данных регионального и федерального уровней (ПТК «ИБД-Р» и ПТК «ИБД-Ф»), а также создания сервиса ИСОД МВД России по формированию, ведению и использованию централизованных оперативно-справочных, криминалистических и разыскных учетов органов внутренних дел Российской Федерации (сервиса «ИБД-М»).

В 2005 - 2007 годах ПТК «ИБД-Р» созданы на основе серверного оборудования, общесистемного и прикладного программного обеспечения, к которому предъявляются жесткие требования по скорости обработки информации и обслуживания запросов пользователей, а также по обеспечению надежности хранения накопленных данных. Всего поставлено и введено в эксплуатацию 94 ПТК регионального уровня. Из них 45 на платформе IBM, 49 на платформе Fujitsu-Siemens.

Использование сотрудниками органов внутренних дел оперативно-справочной, разыскной, криминалистической информации, содержащейся в банках данных федерального и регионального уровня, обеспечивает стабильный рост оперативно-служебных показателей, повышение уровня информационного обеспечения в борьбе с преступностью и охране общественного порядка.

В установленном порядке сотрудникам органов внутренних дел и других ведомств предоставляется доступ к информационным ресурсам ФКУ «ГИАЦ МВД России» и ИЦ. На основе ПТК ИБД-Ф и ПТК ИБД-Р ведется обработка запросов, поступающих по линии ГС ПВДНП, по каналам СМЭВ, а также по линии выполнения государственных услуг (ЕПГУ, МФЦ).

По данным формы 1-ИЦ «Отчет о работе информационных подразделений МВД России за первое полугодие 2018 года», зарегистрировано более 197 тыс. пользователей интегрированных банков данных регионального уровня. Общий объем баз данных («ИБД-Регион») составляет около 37 Тб. В базах данных имеется более 3,5 млрд объектов учета. Информационными центрами отработано более 315 млн запросов (прирост по сравнению с аналогичным периодом прошлого года составляет +64%).

В связи с неуклонным ростом объёма данных ИБДР (в том числе по причине включения фотоизображений в учеты) объёмы хранимых и обрабатываемых данных подходят к пределу паспортных возможностей ПТК.

В результате длительной эксплуатации технологическое оборудование комплексов устарело морально и физически, многие комплектующие сняты с производства, что значительно затрудняет проведение ремонтно-восстановительных работ. Кроме того, даже при наличии некоторых комплектующих работы по ремонту ПТК «ИБД-Р» имеют существенно большую стоимость по сравнению с аналогичными работами на современном оборудовании.

С 13 мая 2016 года в соответствии с совместным решением, утвержденным ФКУ НПО «СТиС» МВД России, ДИТСиЗИ МВД России, ФКУ «ГИАЦ МВД России», ПТК ИБД-Р и «ИБД-Ф» включены в состав ИСОД МВД России и их техническое сопровождение осуществляется в рамках выполнения государственного контракта от 29.01.2016 № 7-2016/НПО (шифр «Эксплуатация изделия 14т1»).

Дополнительным соглашением от 28.03.2017 к указанному государственному контракту предусмотрены работы по поддержанию в установленной степени готовности оборудования и программного обеспечения ПТК «ИБД-Ф» и ПТК «ИБД-Р».

Эксплуатация ПТК «ИБД-Р» осуществляется в соответствии с «Регламентом эксплуатации изделия 14т1», утвержденным 01.07.2017, без увеличения общей стоимости государственного контракта.

В настоящее время ФКУ «ГИАЦ МВД России» согласован подготовленный ФКУ НПО «СТиС» МВД России проект технического задания на оказание услуг по техническому сопровождению эксплуатации ИСОД МВД России, унаследованных систем, программного обеспечения, расположенного в ЦОД ИСОД МВД России, в том числе включающий ПТК «ИБД-Р».

Также во исполнение поручения заместителя Министра внутренних дел Российской Федерации генерал-майора полиции В.Д. Шулики осуществляются мероприятия по тестированию и адаптации работоспособности ППО «ИБД-Р» на современных программно-аппаратных платформах ряда производителей (Huawei, Fujitsu, Lenovo).

По окончании данных мероприятий планируется начать поэтапную замену оборудования ПТК «ИБД-Р» в информационных центрах территориальных органов МВД России на региональном уровне.

Создание сервиса «ИБД-М»

В рамках выполнения ОКР «Развитие ИСОД МВД России» по государственному контракту от 16.12.2014 № 150-2014/ИСОД в 2015 – 2016 годах согласованы и утверждены ФКУ НПО «СТиС» МВД России, ДИТСиЗИ МВД России и ФКУ «ГИАЦ МВД России» техническое задание и технический проект на создание сервиса «ИБД-М». Цель создания сервиса «ИБД-М» — разработка программного обеспечения, позволяющего заменить и впоследствии вывести из эксплуатации ПТК ИБД-Ф, ИБД-Р.

В соответствии с требованиями постановления Правительства Российской Федерации от 27.09.2011 № 797 в 69 субъектах Российской Федерации реализовано электронное взаимодействие МФЦ с МВД России при предоставлении справок о наличии (отсутствии) судимости и (или) факта уголовного преследования, в одном осуществляется тестирование сервиса.

В течение первого полугодия 2018 года через МФЦ посредством сервиса «ИБД-М» подано более 790 тыс. заявлений на получение справок о наличии (отсутствии) судимости, через ЕПГУ - более 980 тыс. На получение

справок об административном наказании за потребление наркотических средств посредством сервиса «ИБД-М» подано более 130 тыс. заявлений.

Одновременно с этим поступает 40-50 тыс. межведомственных запросов ежедневно. При этом более 80 % поступающих запросов автоматически отрабатываются на «да/нет».

Оказание государственной услуги по выдаче справок об административном наказании за потребление наркотических средств, в соответствии с Административным регламентом по предоставлению указанной государственной услуги осуществляется исключительно через ЕПГУ и МФЦ с использованием сервиса «ИБД-М».

С 2015 года проводятся работы по созданию сервиса «ИБД-М». За этот период возникли новые потребности в реализации следующих возможностей сервиса «ИБД-М»:

взаимодействия с внешними информационными системами (например, ГИС ГМП);

совершенствования механизмов предоставления государственных услуг (например, автоматизация подачи заявок на проставление апостиля);

модернизации Межгосударственного информационного банка (в части автоматизации информационного обмена с центральными информационными подразделениями государств-участников СНГ с использованием защищенных каналов связи).

Требуется доработать подсистемы сервиса, обеспечивающие:

конфиденциальность сведений о защищаемых лицах;

аудит действий пользователей;

администрирование;

формирование и ведение централизованного учета граждан, совершивших административные правонарушения и привлекавшихся к административной и уголовной ответственности.

Также предусмотреть разработку программных решений в части работы с «большими данными», позволяющих:

сравнивать различные банки данных;

осуществлять графовый и геоинформационный анализ.

Необходимо определиться с технологической базой, осуществить переход на использование отечественного оборудования и программного обеспечения.

В этой связи результаты работ по созданию сервиса «ИБД-М» следует использовать в качестве научно-технического задела при разработке программного обеспечения, учитывающего современные тенденции и позволяющего в полном объёме заменить и вывести из эксплуатации ПТК ИБД-Ф и ПТК ИБД-Р.

Лекарь Людмила Антоновна,кандидат технических наук,
ведущий научный сотрудник центра систем связи ЦСиСС НИИСТ
ФКУ НПО «СТиС» МВД России

Кондрущенков Олег Михайлович,лейтенант внутренней службы,
научный сотрудник отдела передачи данных ЦСиСС НИИСТ
ФКУ НПО «СТиС» МВД России

Актуальные решения по созданию защищенной ведомственной системы сотовой связи

Для создания защищенной ведомственной системы сотовой связи предлагается использовать современную технологию NGN сетей, ядром которых являются IP-сети, поддерживающие полную или частичную интеграцию услуг передачи речи, данных и мультимедиа различных стандартов. При этом защищенная ведомственная система сотовой связи будет функционировать как VPN (виртуальная частная сеть), наложенная на систему связи общего пользования.

Изначально для передачи различных типов информации строились отдельные (ведомственные) сети связи: телефонная сеть, телеграфная сеть, сети передачи данных и пр. Во второй половине XX века появилась идея объединить все ведомственные сети связи в одну.

Технология NGN - концепция построения сетей связи, обеспечивающих предоставление неограниченного набора услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счет унификации сетевых решений, предполагающая реализацию универсальной транспортной сети с распределенной коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи.

Для сети NGN характерны существенные особенности, выделяющие ее в новый класс телекоммуникационных систем. Обычно выделяют пять таких особенностей NGN:

использование пакетных технологий передачи и коммутации для обмена всеми видами информации;

применение систем коммутации с распределенной архитектурой, которые отличаются от функционально ориентированных телефонных станций;

отделение функций, которые касаются поддержки услуг, от коммутации и передачи;

обеспечение возможности широкополосного доступа и мультисервисного обслуживания трафика вида «triple-play services» (речь, данные и видео);

реализация функций эксплуатационного управления (в том числе и тех, что делегированы пользователям) за счет web - технологии.

На настоящий момент органами государственной власти и силовыми структурами в качестве служебной широко используется сотовая связь в открытом режиме с применением покупных SIM-карт иностранного производства. При этом обмен информацией, местоположение абонентов и другие чувствительные параметры контролируются оператором сотовой связи. Также служебная связь может быть использована сотрудниками и в личных целях.

Транспортная среда на базе сети мобильной связи используется широко, так как создание собственной транспортной среды с учетом требований большой зоны покрытия связи, ее эксплуатация и обслуживание требуют больших организационно-технических затрат. Как показывает практика построения и эксплуатации ведомственных сетей УКВ-радиосвязи, затраты для построения таких территориальнораспределенных систем передачи информации оказываются значительными.

Передача служебной информации в ведомственной системе сотовой связи органами государственной власти и силовыми структурами должна быть защищена сертифицированными программно-аппаратными средствами защиты информации как минимум по уровню «Конфиденциально».

Такая система сотовой связи будет соответствовать системе управления органов государственной власти и силовых структур в отличие от системы сотовой связи общего пользования, где допускается связь каждого с каждым.

Недостатком системы сотовой связи общего пользования является использование ее только в мирное время, и, так как инфраструктура сети принадлежит оператору, сеть может оказаться недоступной при выключении базового оборудования.

Рассматриваемый подход к системе обеспечит требуемый уровень безопасности и скрытности управления силами и средствами органов государственной власти и силовых структур и при этом повысит уровень информационной обеспеченности при выполнении ими задач на уровне, достаточном для принятия ответственных решений, а также повысит оперативность управления процессами и ресурсами в самой VPN сотовой связи [1].

В рассматриваемой системе используются программно-аппаратные средства, обеспечивающие маршрутизацию абонентов в сетях мобильной радиосвязи общего пользования, для организации защищенной связи между существующими разнородными радиосредствами и обеспечения доступа абонентов к информационным ресурсам ведомства.

Все процессы обеспечения защиты информации в VPN на базе системы сотовой связи автоматизированы и происходят под управлением подсистемы автоматизированного управления безопасностью, которая представляет собой комплекс программно-аппаратных средств защиты информации. Подсистема автоматизированного управления безопасностью предназначена для осуществления защиты информации, управления информационным обменом в защищенном режиме, а также для автоматизированного аудита событий безопасности.

Основой построения перспективной системы ведомственной VPN сотовой связи является комплекс технических средств, представленный на рис. 1. В состав рассматриваемого комплекса должны входить доверенная вычислительная среда (ДВС), серверное оборудование (СО) и система идентификация клиентов с возможностью установки ДВС на серверном оборудовании заказывающего подразделения.

В отличие от структуры общедоступной ведомственной системы сотовой связи (связь всех со всеми), в рассматриваемой системе имеется возможность организации иерархии (старший - подчиненный) на уровне каналов связи [2].

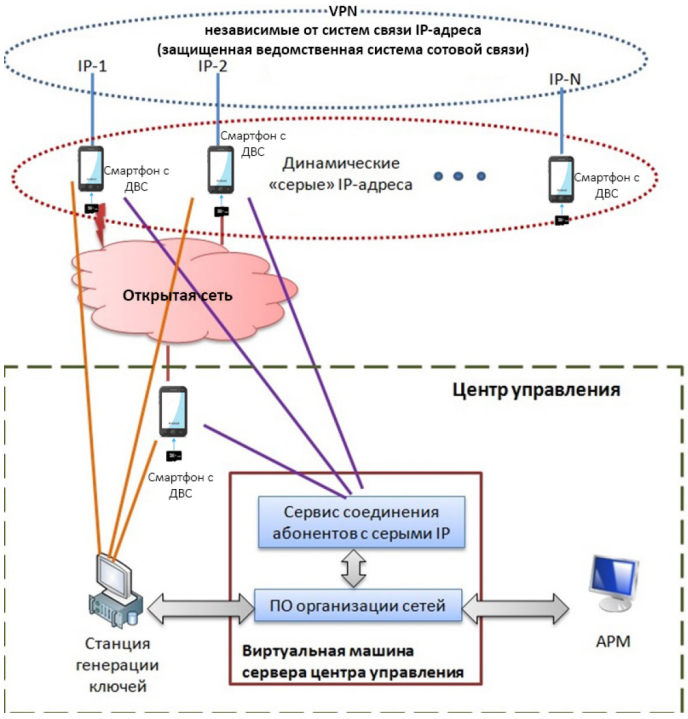


Рис. 1. Общая схема комплекса технических средств

В VPN сотовой связи осуществляется маршрутизация и администрирование трафика каждого абонента, подключенного в сеть общего пользования сотовой связи за счет выделения динамических IP-адресов, обеспечивающих трансляцию сетевых адресов с использованием различных типов сервисов NAT (так называемых «серых» адресов).

Абонентским устройством защищенной VPN ведомственной сотовой связи является любой смартфон под управлением операционной системы Android. Для этого используется специализированное устройство в формфакторе SD или microSD-карт, выполняющее функции ДВС. Доверенной является вычислительная среда, в которой гарантированно отсутствуют незадекларированные возможности. Перспективным является использование такой ДВС, реализованной в микроэлектронном исполнении.

Предлагается использовать микроэлектронное устройство российской разработки со следующими характеристиками:

современные криптографические алгоритмы;

производительность в режимах криптографической обработки информации - от 1 Мбит/с до 1 Мбайт/с;

объем встроенной памяти - до 32 Гбайт;

возможность загрузки доверенной операционной системы;

совместимость практически со всеми современными мобильными платформами, такими как смартфоны, планшеты;

наличие режима «sleep» с уменьшенной потребляемой мощностью.

ДВС на базе микроэлектронного устройства является отчуждаемым элементом, и смартфон может быть сертифицирован как конфиденциальное устройство в объеме объекта корректности встраивания.

В соответствии с возможностями специализированного устройства в формфакторе SD или microSD-карт в смартфон встраивается отечественная операционная система реального времени (ОС РВ), выполняющая в соответствии с требованиям обмена в ведомственной системе сотовой связи необходимый объем функций из числа поддерживаемых операционной системой Android.

Смартфон как абонентское устройство защищенной ведомственной сети связи должен отвечать следующим техническим требованиям:

защищенный режим смартфона обеспечивается после перезагрузки. В открытом режиме смартфон представляет собой бытовой сотовый телефон;

средства защиты информации реализуются в микроэлектронном исполнении в ДВС. Смартфон работает в защищенном режиме на базе ОС РВ;

ВС исполняется в формфакторе SD или microSD-карты для смартфона и является отчуждаемым элементом.

ОС РВ должна функционировать в ДВС на базе микроконтроллера «Курган», имеющего следующие характеристики:

производительность в режимах криптографической обработки информации - от 1 Мбит/с до 1 Мбайт/с;

объем встроенной памяти - до 32 Гбайт;

возможность загрузки доверенной операционной системы.

Современная ОС РВ отечественной разработки специализирована под задачи применения в составе смартфона. ОС РВ – это разновидность операционных систем, обеспечивающих требуемую функциональность в заданный промежуток времени.

Отличительной особенностью ОС РВ является то, что она создается «с нуля» целенаправленно под задачи применения в составе защищенных технических средств, где имеется необходимость надежного решения проблем информационной безопасности. Также ОС РВ может функционировать на различных вычислительных платформах, что подтверждено практикой. Если изначально она создавалась только на платформу с ARM-архитектурой, то на настоящее время ОС РВ успешно применена на платформе с архитектурой Intel X86. ОС РВ представляет собой полноценную операционную систему с рядом необходимых библиотек.

Создаваемая система связи имеет собственную логическую инфраструктуру управления, которая не зависит от зарубежных ресурсов и комплексно реализует современные технологии связи на основе построения NGN сетей в отечественных элементной базе и ОС РВ.

СПИСОК ЛИТЕРАТУРЫ

1. Кондрущенков О.М., Лекарь Л.А. Построение защищенного ведомственного портала// Информационная безопасность социотехнических систем. 2017. № 3 (1). С. 32– 37.

2. Кондрущенков О.М., Лекарь Л.А. Защищенная территориально-распределенная мультисервисная система связи для обеспечения управления в реальном масштабе времени// Информационная безопасность социотехнических систем. 2017. № 1 (1). С. 53– 58.

Пузарин Андрей Валерьевич, начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России им. В.Я. Кикотя

Реализация компетентностного подхода к подготовке сотрудников органов внутренних дел в свете современных вызовов и угроз

Происходящие в мире и в нашей стране изменения в характере образования все более явно ориентируют его на «свободное развитие человека», на творческую инициативу, самостоятельность, конкурентоспособность, мобильность будущих специалистов. Соответственно изменения в области педагогических целей обуславливают необходимость обеспечения образованием более полного, личностно и социально интегрированного результата. В качестве общего определения такого интегрального социально-личностно-поведенческого феномена, как результат образования, в совокупности мотивационно-ценностных, когнитивных составляющих и выступило понятие «компетенция/компетентность». Это означает формирование новой парадигмы результата образования.

Компетентностный подход - это совокупность общих принципов определения целей образования, отбора содержания образования, организации образовательного процесса и оценки образовательных результатов. К числу таких принципов относятся следующие положения:

смысл образования заключается в развитии у обучаемых способности самостоятельно решать проблемы в различных сферах и видах деятельности на основе использования социального опыта, элементом которого является и собственный опыт учащихся;

содержание образования представляет собой дидактически адаптированный социальный опыт решения познавательных, мировоззренческих, нравственных, политических и иных проблем;

смысл организации образовательного процесса заключается в создании условий для формирования у обучаемых опыта самостоятельного решения познавательных, коммуникативных, организационных, нравственных и иных проблем, составляющих содержание образования;

оценка образовательных результатов основывается на анализе уровней образованности, достигнутых учащимися на определённом этапе обучения.

Компетентностный подход предполагает не простую трансляцию знаний, умений и навыков от преподавателя к обучаемым, а формирование профессиональной компетентности.

В свете современных вызовов и угроз видится целесообразным формирование профессиональных компетенций сотрудника органов внутренних дел, связанных, в том числе, с информационными технологиями, с обеспечением безопасности информации при их использовании.

Иными словами, основной целью профессионального образования является подготовка квалифицированного сотрудника соответствующего уровня и профиля, компетентного, свободно владеющего своей профессией и ориентирующегося в смежных областях деятельности, готового к постоянному профессиональному росту, социальной и профессиональной мобильности.

В область профессиональной деятельности выпускников, освоивших программу специалитета, необходимо включить такие компетенции, как:

способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации;

способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах;

способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;

способность применять технические и программно-аппаратные средства обработки и защиты информации.

Формирование перечисленных компетентностей происходит на теоретическом уровне, но основная их часть формируется на практике с использованием лабораторий, полигонов и.т.д.

Отдельной проблемой является обучение как действующих сотрудников, так и курсантов работе на Astra Linux Special Edition по реализации требований безопасности информации.

Мандатное разграничение доступа

Изоляция модулей

Очистка оперативной и внешней памяти и гарантированное удаление файлов

Маркировка документов

Регистрация событий

Механизмы защиты информации в графической подсистеме

Режим ограничения действий пользователя (режим «киоск»)

Защита адресного пространства процессов

Механизм контроля замкнутости программной среды

Контроль целостности

Средства организации домена

Защищенная реляционная СУБД

Защищенный комплекс программ электронной почты

Защищенный комплекс программ гипертекстовой обработки данных

Захаров Дмитрий Никанорович,
старший лейтенант полиции,
доцент кафедры СИТ УНК ИТ МосУ МВД России им. В.Я. Кикотя
кандидат технических наук

Практические аспекты подготовки специалистов в области информационной безопасности для органов внутренних дел с учетом требований цифровой экономики

Цифровая экономика предъявляет новые требования к субъектам, в ней участвующим. Обеспечение информационной безопасности, защиты компьютерной информации, защищенности сведений, составляющих охраняемую законом тайну, расследования преступлений в сфере информационных технологий и иные подобные проблемы, напрямую связанные с обеспечением национальной безопасности государства, защитой конституционных прав и свобод граждан, стоят особенно остро.

Московский университет МВД России имени В.Я. Кикотя, как головное образовательное учреждение в системе образования Министерства, должно поддерживать высочайший уровень образования, постоянно актуализируя дидактические единицы читаемых дисциплин с учетом новых реалий. Имеется серьезный дефицит кадров в образовательном процессе всех уровней образования.

В сложившейся обстановке Министром внутренних дел Российской Федерации определена задача - организовать качественную подготовку специалистов в области расследования киберпреступлений на основе утвержденной в июле 2017 г. распоряжением Правительства Российской Федерации программы «Цифровая экономика». В социально-экономических условиях принятия программы указано, что существует серьезный разрыв в цифровых навыках между отдельными группами населения. Данный тезис обуславливает задачу правоохранительных органов по противодействию преступности в сфере высоких технологий, направленной на группы населения, не осведомленные о совместном уровне компьютерных технологий.

В целях решения поставленной задачи при формировании компетенций, предусмотренных образовательными стандартами, а также при реализации практико-ориентированного подхода к обучению в июле 2016 года между ПАО «Сбербанк» и Московским университетом МВД России имени В.Я. Кикотя подписано соглашение о стратегическом партнерстве в области подготовки кадров по борьбе с киберпреступностью. В рамках данного соглашения на базе Сбербанка с курсантами и слушателями университета проведен курс учебных занятий в объеме 80 часов по изучению уязвимостей банковских систем и механизмов следообразования совершаемых киберпреступлений. Для проведения занятий были приглашены ведущие специалисты по кибербезопасности в различных областях компьютерных технологий.

В настоящее время реализуется второй этап обучения курсантов на базе центра противодействия кибермошенничеству ПАО «Сбербанк», в рамках которого создано несколько учебных следственно-оперативных групп по 2 курсанта из каждого профильного подразделения университета, в которых при участии специалистов центра курсанты занимаются отработкой учебных заявлений, составленных по типовым преступлениям в финансово-кредитной сфере, с составлением документов, соответствующих своему профилю. По завершении этого курса будет проведен второй этап – «киберучения», на основе которого конкурсная комиссия определит лучшую учебную следственно-оперативную группу.

Кроме того, на базе учебно-научного комплекса информационных технологий в Московском университете МВД России имени В.Я. Кикотя при поддержке ПАО «Сбербанк» развернуты «Лаборатория информационной безопасности в экономической сфере (информационной безопасности банковских продуктов)», полигон расследования инцидентов в области компьютерной безопасности, лаборатория по изучению технологии блокчейн и криптовалют.

На базе института подготовки сотрудников для органов предварительного расследования создан полигон «Отделение банка», в котором оборудованы типовой офис банка и ряд учебных мест.

По линии повышения квалификации и переподготовки кадров университет осуществляет работу с сотрудниками подразделений уголовного розыска, экономической безопасности и противодействия коррупции, следователями, специализирующимися на расследовании преступлений в сфере компьютерной информации, совершаемых против собственности регионального и районного уровней.

На базе университета существует несколько команд, одна из которых участвует в соревнованиях по компьютерной безопасности – CTF. В них отобраны лучшие курсанты и слушатели по результатам промежуточных аттестаций. В рамках договора о сотрудничестве между университетом и МГУ им. М.В. Ломоносова члены команды посещают спецсеминары по «Основам защиты программного обеспечения», «Цифровой криминалистике», «Windows Kernel Exploitation» на базе факультета Вычислительной математики и кибернетики.

Для повышения качества практико-ориентированного подхода по линии подготовки специалистов по специальности «Судебная компьютерная экспертиза» между университетом и АО «Лаборатория Касперского» заключено соглашение о сотрудничестве. Специалисты лаборатории взаимодействуют с профессорско-преподавательским составом в методическом наполнении специальных дисциплин, связанных с компьютерной экспертизой.

В целях повышения заинтересованности курсантов и слушателей на базе учебно-научного комплекса информационных технологий ежегодно проводится шесть научно-представительских мероприятий всероссийского уровня, профильных практических подразделений, на которые приглашаются сотрудники, а также представители ведущих российских компаний в области информационных технологий.

Серезевский Алексей Вадимович, старший преподаватель
кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России им. В.Я. Кикотя,
кандидат технических наук, подполковник полиции

Парадигма повышения качества решения задач по снижению аварийности на дорогах с помощью цифровых устройств нового поколения

В повседневную практику правоохранительных органов внедряется значительное количество технических средств самого разного назначения. Применение технических средств в деятельности органов внутренних дел, как и в любой другой, позволяет увеличить эффективность работы, решать различные практические задачи меньшим количеством сотрудников.

Федеральный закон «О полиции» обязывает полицию использовать в своей деятельности достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру. Применяются технические средства противодействию преступности, как в охране общественного порядка, так и в повседневной и обеспечивающей деятельности. Невозможно представить функционирование системы управления без современной системы связи, оперативно-разыскную деятельность без оперативной техники, повседневную деятельность сотрудника без современной оргтехники и т.д. Такие примеры можно привести для всех направлений и сфер деятельности органов внутренних дел.

Технические средства, применяемые в ОВД, в основном автоматизируют труд полицейского. Но есть и состоящие на вооружении полностью автоматические средства, решающие, например, задачи по предупреждению административных правонарушений на автомобильных дорогах. Современная автоматика, естественно, использует законы физики в совокупности с новейшими достижениями в области инфокоммуникационных технологий, которые в обиходе называют цифровыми.

Так что же представляет собой «цифровой полицейский»? Каково его предназначение? Какие задачи он должен решать? Обратимся к первоисточнику. Закон «О полиции» чётко определяет цели и функции полиции в целом, на которые и опираются разработчики и технические специалисты. Таким образом, к «цифровым полицейским» можно отнести автоматические технические средства и системы, которые в той или иной мере способствуют решению законодательно закрепленных за полицией задач.

Рассмотрим одну из проблемных областей, которая в настоящее время решается с привлечением «цифровых полицейских» – снижение аварийности на автомобильных дорогах путём контроля скорости транспортных средств.

Следует отметить тот факт, что ежегодные экономические потери нашей страны от аварий составляют около 2-х процентов ВВП, ведь треть погибших в авариях – это наиболее активные граждане в возрасте от 25 до 40 лет. В подписанном в этом году президентом указе «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» предлагается снизить смертность при ДТП до нулевого уровня к 2030 году. Правительством России разработан проект по созданию безопасных и качественных автомобильных дорог исходя из того, что в 2024 году смертность в результате ДТП нужно снизить в 3,5 раза по сравнению с 2017 годом.

В настоящее время задача контроля скорости более-менее успешно решается путём установки комплексов фотовидеофиксации.

Рис. 1. Комплекс фотовидеофиксации «Стрелка-СТ»

Обилие видеокамер заставило многих водителей кардинально пересмотреть свое поведение на дороге, т.е. наблюдается положительный эффект от их применения. До 2024 года количество таких комплексов на российских дорогах необходимо увеличить вдвое, такова позиция Минтранса. Сейчас в России насчитывается свыше 9 тысяч стационарных, 3,8 тысячи передвижных и 656 мобильных комплексов автоматической фиксации нарушений. Также в данном ведомстве планируют динамически перераспределять расположение камер. Например, перенос комплексов на новые участки и установка на их месте муляжей помогут сэкономить бюджетные средства.

Здесь необходимо акцентировать внимание на следующем факте: установка и обслуживание данных систем отданы в частные руки. Бизнесмены заключают с властями контракты на оборудование дорог стационарными и мобильными комплексами фотовидеофиксации, а также на их обслуживание. И с каждого выписанного штрафа получают определенную сумму.

Данный опыт послужил для формирования следующего предложения: проработать с технической и организационной точек зрения вопрос установки комплексов фотовидеофиксации на движущиеся транспортные средства - маршрутные или частные. Такие комплексы должны определять собственную скорость (применяя эффект Доплера), максимально разрешенную скорость на данном участке автодороги (используя системы GPS или ГЛОНАСС в совокупности с автоматическим считыванием и распознаванием дорожных знаков), а также скорости встречных и попутных транспортных средств и на основе этой информации делать вывод о правонарушениях, фиксировать их, накапливать данные и отправлять по защищенным каналам связи в центры обработки. Для компенсации затрат на покупку, установку, обслуживание такой техники, а также в целях формирования личной заинтересованности автопаркам и частным лицам предлагается с каждого уплаченного штрафа перечислять небольшой процент.

Рис. 2. Мобильные программно-аппаратные комплексы автоматической фиксации правонарушений для патрульных автомобилей

Существующие комплексы фотовидеофиксации, показавшие высокие результаты эксплуатации, предлагается взять за основу и модернизировать, минимизировав их габаритные размеры, в том числе и за счёт изменения рабочей частоты, а также проработать вопросы уменьшения негативного влияния электромагнитного излучения, введения дополнительных функциональных модулей и переработки программного обеспечения. Всесторонне рассмотреть эти вопросы можно в рамках соответствующей научно-исследовательской работы и, при положительных результатах исследования, последующей опытно-конструкторской работы.

Далее хотелось бы обратить внимание на следующий аспект. По отчетам Госавтоинспекции, число оштрафованных за нарушения ПДД из года в год почти не меняется. То есть водители нарушают правила регулярно. При этом размер штрафа зачастую не имеет принципиального значения, и злостными нарушителями являются владельцы с высоким уровнем дохода. Для некоторых из них рамок не существует и возникает ощущение вседозволенности. Поэтому штрафные санкции, как правило, оказываются эффективными в основном по отношению к законопослушным гражданам.

В качестве решения данной проблемы можно рассмотреть следующее. Сама идея не нова и заимствована из практического опыта некоторых стран.

Рис. 3. «Умный лежачий полицейский»

Нарушитель, который не боится штрафов, в большинстве случаев будет беречь свой автомобиль, поэтому предлагается вкупе с комплексами фотовидеофиксации использовать так называемых «умных лежащих полицейских», которые при превышении скорости образовывают небольшие выпуклости и/или впадины на дорожном полотне на полосе нарушителя. Такое точечное воздействие на нарушителя не помешает добропорядочным автовладельцам. Это достаточно дорогое, но эффективное с точки зрения контроля скоростного режима техническое средство.

Хотелось бы остановиться и на следующем факте. Многие используют так называемые антирадары, которые на основе улавливаемого сигнала от комплекса фотовидеофиксации предупреждают водителя. Таким образом, он соблюдает скоростной режим только в области видимости камеры, а в остальных случаях не обращает на него особого внимания, что сводит на нет всю дорогостоящую идею внедрения камер на дорогах. В качестве решения предлагается используя существующие вышки, максимально покрыть площадь автодорог радиомаяками, благодаря которым антирадары выдавали бы постоянный сигнал контроля скорости, нарушая этим их основной функционал. В дополнение к этому предлагается расставить большое количество муляжей видеокамер. Данные меры являются более бюджетными по сравнению с увеличением числа реальных камер на дорогах. Радиомаяки предлагается разработать самозаряжающимися от естественных источников света, необслуживаемыми и с автоматической передачей по радиоканалу в центр управления сигналов об их работоспособности.

Для гарантированного контроля скорости можно рассмотреть еще одно предложение - разработку технической системы, устанавливаемой на автомобили. Эти системы смогут принудительно ограничивать скорости транспортных средств на различных участках автодорог с учётом спутниковых сигналов систем GPS и/или ГЛОНАСС в совокупности с автоматической системой считывания дорожных знаков. Их применение значительно повысило бы безопасность на дорогах. Подобные системы уже существуют в упрощенном виде. Это так называемые устройства ограничения скорости автомобиля - специальный механизм, предотвращающий превышение скорости транспортным средством сверх заранее установленных значений. Установка таких устройств обязательна для всех автомобилей грузоподъемностью более 3,5 тонны, которые задействуются при перевозке опасных грузов.

В заключение хотелось бы отметить следующее. Минпромторг России заявляет о разработке к 2020 году технологий, обеспечивающих обнаружение пешеходов, препятствий и транспортных средств в условиях ограниченной видимости. По сути, речь идет о создании системы экстренного торможения перед препятствием с функцией распознавания пешеходов. Она уже доступна на некоторых моделях автомобилей импортного производства, а через несколько лет станет обязательной для базового оснащения автомобилей, продающихся на европейском рынке.

Рис. 4. Система экстренного торможения перед препятствием с функцией распознавания пешеходов

Такая система, если она будет создана и покажет свою эффективность, по праву сможет именоваться «цифровым полицейским», решая задачу по предупреждению преступлений и правонарушений на автодорогах.

Копин Вадим Викторович,
директор ООО «Хайскрин Смарт»

Внедрение инновационных проектов в структурах МВД России

Современный технологический процесс создания мобильных гаджетов для больших корпораций или крупных государственных организаций включает несколько этапов. Среди них можно выделить два основных:

создание самого гаджета и программного обеспечения к нему;

создание клиент-серверной системы с распределенным уровнями доступа, хранения и алгоритмами обработки полученной информации.

Создание таких систем для спецслужб, безусловно, связано с прохождением спецсертификации.

На сегодняшний день компания «Хайскрин Смарт» работает над первым этапом. Подобные проекты имеют определенную специфику: главная трудность в их реализации состоит в отсутствии формальных требований к устройству у потенциального заказчика. Поэтому первейшей задачей является создание фокус-групп, состоящих из представителей заказчика и разработчика.

Предусматривают следующие этапы разработки и внедрения:

• На первом этапе мы совместно с заказчиком определяем задачи и возможности их реализации, основываясь на современных технологиях и методиках производства. В данном случае положительным фактором является возможность привлечения специальных экспертов, доступных только для заказчика. Этап занимает от 2 недель до месяца.

• Далее происходит разработка самого устройства (его спецификации, механического дизайна, условий эксплуатации и опытной трехмерной модели) с непосредственным участием заказчика. Корректируется или разрабатывается необходимое мобильное программное обеспечение. Все это позволяет создать не выставочный образец, который хорошо выглядит, но не выполняет заявленных функций, а полноценный инструмент, помогающий в работе. Обычно этот этап занимает от 3 до 5 месяцев.

• Третий – один из важнейших этапов сертификация. При гражданском применении гаджета этот процесс занимает до 2 месяцев и стоит недорого, при специальном использовании около 2-х лет. Накладные расходы при этом велики. Это, как представляется, самая большая проблема. Без ее решения заказчик никогда не получит продукт, отвечающий необходимым требованиям. Современная скорость построения электроники и связи велика. Полная замена применяемых технологий происходит не реже одного или более раз в год. Причем зачастую эти изменения абсолютно революционны (например, переход с 4G на 5G в следующем году).

• На четвертом этапе осуществляется закупка необходимых комплектующих, их транспортировка и сборка гаджетов под контролем заказчика на мощностях российского предприятия. Это занимает от 1 недели до 1 месяца, в зависимости от конструктивной сложности устройств и их количества.

• Пятый этап-отгрузка продукции заказчику.

• Гарантийное/пост-гарантийное обслуживание и сопровождение.

Для достижения задач, поставленных перед структурой МВД России, в целях реализации концепции «Цифровой полицейский» необходимо создание совместной рабочей группы с институтами Министерства и специалистами компании-разработчика.

Главный постулат – сотрудники МВД России как эксперты знают, что им необходимо для выполнения своих задач. Задача компании-помочь систематизировать и спроектировать необходимый набор гаджетов, предложив свои опыт и знания.

Как результат взаимодействия, за короткое время (5-7 месяцев) мы получим качественную разработку любой сложности и быстро произведем необходимое количество оборудования. Причем производство можно разместить на мощностях нашего партнера госкорпорации ТВЭЛ. Предварительное согласие от него уже получено.

Важно отметить также, что время прохождения спецсертификации не должно быть таким долгим, так как специалисты МВД России будут принимать непосредственное участие в создании и проектировании, и смогут совместно с компанией-разработчиком предоставить все необходимые материалы в сертификационные органы.

Копин Вадим Викторович,
директор ООО «Хайскрин Смарт»

Перспектива развития мобильной электроники в концепции «Электронный полицейский»

Нательный видеорегистратор

Устройство оснащено ИК-подсветкой, что позволяет вести видеозапись в условиях низкой освещенности. Наряду с видео происходит автоматическая запись трека со встроенного приемника ГЛОНАСС. Регистратор оснащен сенсорным ЖК-экраном. Помимо стриминга видео через LTE, пользователь может загружать данные на сервер через специальные терминалы. Одной из ключевых особенностей является выделенная кнопка SOS для немедленного оповещения центра управления об опасности.

- Поддержка LTE: видеостриминг и удаленное управление.
- HD/FHD Видео (720p/1080p)
- Более 6 часов в режиме видеосъемки
- Широкоугольная линза (105°)
- Работа в режиме рации на базе защищенного облака
- Режим ночной съемки
- Геопозиционирование посредством GPS/GLONASS
- Прочный IP67-защищенный корпус

Топология предлагаемого решения Интегрированное решение:

предоставляет доступ к видеозаписи на абонентских терминалах в режиме реального времени;

позволяет отслеживать местоположение абонентских терминалов в режиме реального времени;

осуществляет передачу голосовых сообщений на абонентские терминалы;

реализует функцию рации на основе защищенного облачного сервиса;

осуществляет сбор и классификацию собранных данных.

Возможна дальнейшая интеграция с сервисами компании NTech Lab для распознавания лиц в толпе по заданным признаками в режиме реального времени.

Патрульный жезл

С поддержкой LTE и HD фото/видеосъемки

Быстрый восьмиядерный процессор, Android 7.1

Обеспечивает мгновенный отклик и плавную работу системы и фото-видеосъемки.

Два диапазона 2.4G/5G | Bluetooth 4.2 | GPS/ГЛОНАСС

Аккумулятор повышенной емкости: 10000 мА·ч

Устройство может непрерывно работать до 10 часов при включенной камере и подсветке одновременно, до 20 часов съемки при выключенной подсветке и до 1 месяца в режиме ожидания.

Поддержка всех видов сетей. Стриминг видеоизображения.

- Поддержка большинства диапазонов
- Поддержка двух сим-карт
- Поддержка 2G/3G/4G сетей

TELE2, МТС, МегаФон, Билайн

USB Type-C: быстрая зарядка и двусторонний коннектор

- **Qualcomm QuickCharge 3.0 – менее 4 часов до 100%**
- **Порт водонепроницаем даже без защитной крышки**

Многофункциональный гаджет для спецслужб

- Мощный фонарь
- Прожектор
- Микрофон
- Динамик
- Красный и зеленый сигналы
- Лазерный прицел

16.0MP HD Камера

- Большая апертура (F2.0)
- Высокая светосила
- FHD Видео (1080p)
- 5-линзовая оптика
- PDAF высокоскоростной автофокус