ЛОГИСТИКА НА АВТОПИЛОТЕ

Артур Мурадян, эксперт рабочей группы Госдумы по законодательному регулированию беспилотного транспорта и генеральный директор транспортной компании Traft, рассказывает о двух аспектах инновационного транспорта и программного обеспечения – положительном и том, который требует повышенного внимания во избежание грядущих проблем.

Артур Мурадян,
генеральный директор транспортной компании Traft

Осенью прошлого года правительство одобрило поправки в КоАП, которые разрешают принимать в качестве официального доказательства нарушений водителем ПДД фотографии и видеозаписи, сделанные очевидцами. Параллельно в рабочей группе комитета по транспорту Государственной думы завершается подготовка проекта по введению полного перечня правовых аспектов, связанных с опасным вождением. Данные решения имеют основополагающее значение для дальнейшего развития систем сбора больших данных в транспорте.

До недавнего времени сбор данных, которые могут котироваться в судах при разборе обстоятельств различных аварий, имел жесткую вертикальную интеграцию. Например, далеко не всегда принимались к рассмотрению данные с видеокамер, установленных на дорогах общего пользования. Существующие регламенты видеофиксации нарушений во всем мире имеют ограниченный перечень ситуаций, подпадающих под определение нарушений ПДД. Проблема в том, что сценариев поведения транспортных средств на дороге, особенно в перспективе появления на трассах первых беспилотников, куда больше, чем заложено в электронные алгоритмы камер. На данный момент это создает большую погрешность при использовании данных. В Нидерландах, например, ежегодно фиксируется около 1,5 млн ДТП, но полицией учитывается не более 300 тыс. В этой связи поправки в КоАП существенно улучшают сложившуюся ситуацию.

Дополнительно помогут беспилотники. Речь идет о планомерном распространении систем машинного зрения и беспилотных автомобилей, оснащенных системой интеллектуальной видеофиксации нарушений общественного правопорядка. Уже существующие сегодня системы машинного зрения и беспилотного управления автомобилями позволяют в режиме реального времени распознавать траекторию и характер движения автомобилей по дорогам общего пользования. При идентификации любых резких перестроений система анализирует дорожную сцену, внутри которой происходит подобная ситуация, при этом учитывается дорожная разметка, соответствие скорости машины ограничениям на данном участке дороги, средняя скорость потока, плотность движения, тип дороги, время суток, погодные условия (гололед, туман).

В случае выявления опасного вождения беспилотный автомобиль, не спеша в потоке патрулирующий российские дороги, с помощью своей оптической системы распознает номера лихача (а также его характерные признаки – тип кузова, цвет) и затем передает информацию о нем с учетом ГЛОНАСС-локации на ближайший пункт ДПС, чтобы машину немедленно остановили для проверки.

В то же время не стоит забывать, что стремительное проникновение информационных систем в отрасль транспорта и грузоперевозок приводит к появлению целых направлений по противодействию оцифровке логистики и новым видам технологического мошенничества. Пока есть те, кто хочет сделать перевозки автоматизированными и прозрачными, будут и те, кто видит в этом угрозу для своих действий по ма-

нипуляции отчетными документами с целью колоссальных дополнительных заработков. Статистически установлено, что в ценнике на любую автомобильную перевозку в России до 30% стоимости уходит на приписку водителями времени, которое они якобы потратили на рейс. Точечное воздействие на одну лишь эту зону сэкономит миллиарды рублей частных и государственных бюджетов ежегодно. К счастью, системы мониторинга грузоперевозок в нашей стране развиваются стремительно и данный вопрос рано или поздно будет полностью решен.

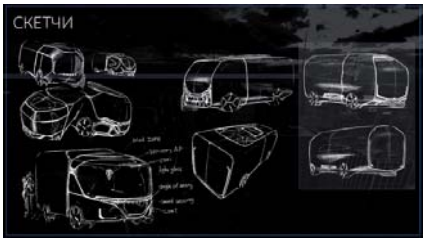
Статистически установлено, что в ценнике на любую автомобильную перевозку в России до 30% стоимости уходит на приписку водителями времени, которое они якобы потратили на рейс. Точечное воздействие на одну лишь эту зону сэкономит миллиарды рублей частных и государственных бюджетов ежегодно.

Но приписка времени – лишь одно звено в длинной цепи мошеннических действий. Воздействовать нужно на всю цепь, в противном случае подавление действий на одном фронте будет провоцировать всплеск активности на другом. Даже в эру блокчейна и больших данных грузоперевозка не защищена от банального грабежа, который многие перевозчики и их клиенты не смогут обнаружить до прибытия в место назначения. Так, злоумышленники уже научились печатать точные копии пломб на 3D-принтере… Такая процедура занимает несколько минут и помогает полностью скрыть следы проникновения в кузов, что максимально усложняет процесс выявления времени и места совершения преступления. При условии длительной междугородней перевозки этот факт может повлиять на подачу документов в правоохранительные органы – не будет четкого понимания в чьей юрисдикции произошел инцидент.

В свою очередь, периодически появляющиеся в СМИ новости об очередной успешной попытке взлома системы «Платон» убеждают и в том, что современные мошенники в логистике будут пытаться взламывать сами транспортные системы или мобильные устройства с приложениями, которые устанавливают водители, чтобы постоянно быть на связи с перевозчиком и подавать сигнал о своих передвижениях через GPS. На хакерском рынке давно получили активное хождение программы и аппаратные комплексы для перехвата и проецирования ложного сигнала GPS, чтобы запутать, например, того, кто использует спутниковые сигналы для контроля перевозок.

Все это подводит нас к мысли о том, что в сфере логистики обязательно должны быть разработаны собственные лицензии по обеспечению безопасности транспортного программного обеспечения (ПО). Эти документы на уровне лицензий ФСТЭК должны обязывать каждого разработчика создавать обязательные уровни защиты для своего транспортного ПО. Требования должны быть сухими, жесткими, с обязательными штрафами за их нарушение. Причина такого подхода до боли проста. Ни одно ПО на рынке технологически не может существовать как «вещь в себе» и не допускать в свой периметр безопасности сторонние универсальные решения. Слабое звено – тот самый GPS-передатчик и сам мобильный телефон водителя с мобильной версией транспортного ПО. Если водитель получает заказы на перевозки у двух и более компаний и использует для их выполнения разные мобильные клиенты транспортного ПО, то хакеры, удаленно взломав мобильный телефон водителя, сразу же получают доступ к его аккаунтам во всех логистических системах. Это каскадная зависимость технологий и устройств, и важно не допустить цепной реакции в случае хакерской атаки.

К сожалению, многие современные разработчики транспортного ПО, да и сами логистические компании слишком ослеплены модной уберизацией и не просчитывают последствия так далеко, как необходимо. Очень хотелось бы, чтобы в случае с данной проблемой наши коллеги научились решать ее заочно, не доводя до «собственного опыта», потому что такой личный пример одной компании может тут же стать последним для всех.



Работы студентов пяти российских вузов в рамках Международного конкурса на лучший дизайн беспилотного автомобиля, который был проведен в 2017 году