

Информационные технологии

Компьютеризированная система контроля трафика на крупных предприятиях (система «Цербер»)

Н. А. АБРАМОВ

Аннотация. В данной статье рассматриваются технические средства для предотвращения краж на крупных предприятиях, в частности — комплексные системы видеонаблюдения. Описаны плюсы и минусы различных систем, приводится описание системы «Цербер». Описаны алгоритмы, лежащие в основе данной системы, такие как алгоритмы частичной прецедентности, используемые для распознавания номеров, а также алгоритм проверки легитимности действий водителя.

Ключевые слова: видеонаблюдение, машинное зрение, распознавание образов, алгоритмы частичной прецедентности, выявление краж, информатизация предприятий, управления предприятием.

Введение

Одной из основных проблем, которую приходится решать руководителям предприятий в России, является обеспечение сохранности производимой продукции. В настоящее время хищение продукции носит массовый характер и в основном направлено на кражу конечной продукции предприятия. Экономический ущерб от хищений колоссален, вплоть до того, что в стоимость продукции изначально закладываются значительные издержки, связанные с кражами. В России эта ситуация обострена низким уровнем жизни рабочих, плохими условиями труда и слабым внедрением систем защиты от хищений.

Для борьбы с хищениями используются различные меры: наем частных охранных компаний, создание систем контроля доступа, различные системы пропусков и т. д. Но, к сожалению, большинство из них опирается в той или иной мере на человеческий

фактор, а, как известно, самым слабым звеном любой системы является человек.

В случае крупных промышленных заводов поток машин, проходящий через территорию завода за сутки, огромен, и отследить каждую из них сложно без комплексной системы видеонаблюдения/контроля. При этом стоимость продукции, вывозимой на одной машине, может достигать нескольких сотен тысяч долларов, и кража даже с помощью одной машины может нанести значительный финансовый ущерб. Также территории таких промышленных компаний обычно весьма велики, и осуществлять контроль только с помощью людей экономически нецелесообразно, поскольку потребуются сотни сотрудников охраны.

Воры — весьма изобретательные люди. Например, часто из уже груженной выезжающей машины часть продукции прячется где-то на территории завода (например, закапывается), и машина подъезжает к цеху уже частично разгруженной, а продукцию по

частям и постепенно вывозят на других машинах. Однако для проведения такой операции машина должна провести достаточно много времени на территории завода, что обычно не отслеживается на российских предприятиях. Также иногда используются специальные подставные машины с поддельными документами, пропусками и номерами.

Тем не менее в случае завода размер продукции обычно достаточно велик, и вывезти ее, кроме как на грузовом автомобиле, не представляется возможным. Поэтому основная задача системы безопасности — обеспечить контроль над вывозом продукции на грузовых автомобилях.

1. Системы видеонаблюдения

Чтобы справиться с растущими требованиями к системам видеонаблюдения, проводится большой объем исследований, для улучшения существующих и разработки новых решений в сферах обработки сигналов, коммуникаций, инженерных систем и машинного зрения. Внедряемые системы видеонаблюдения как правило используют стандартное оборудование в них все чаще применяются программные средства для обработки сигналов, поступающих из видеокамер. Одними из основных задач для этих систем, являются распознавание несанкционированных вторжений и перемещений объектов, а также обнаружение подозрительных предметов [4].

Академические исследования в этой области в основном сосредоточены на улучшении алгоритмов обработки изображений, что позволяет создавать методы более точного и надежного обнаружения и распознавания объектов, слежения за объектами, распознавания человеческой активности. Кроме того проводятся разработки по созданию СУБД для систем видеонаблюдения и инструментов оценки эффективности систем видеонаблюдения. Другие исследования в настоящее время проводятся с целью поиска новых решений для передачи видеoinформации в распределенных системах видеонаблюдения. Примерами таких решений являются методы сжатия видео, построение сетей и протоколов передачи данных, распределение задач обработки и стандарты форматов данных для передачи по сети.

Внедрение систем видеонаблюдения началось с аналоговых систем CCTV (closed-circuit television — телевидение замкнутого контура). Эти системы состоят из нескольких камер, расположенных в нескольких местах и связанных с набором мониторов, которые обычно помещаются в одну контрольную комнату в виде «матрицы мониторов». В настоящее время большинство систем CCTV используют аналоговые технологии для передачи и хранения изображений. Обычные камеры видеонаблюдения ис-

пользуют для захвата изображений цифровые ПЗС-матрицы. Цифровое изображение преобразуется в аналоговый композитный видеосигнал, который связан с мониторами и записывающим оборудованием CCTV, и передается, как правило, через коаксиальный кабель. Цифро-аналоговое преобразование вызывает ухудшение качества картинки, а аналоговый сигнал чувствителен к шуму. Можно улучшить системы видеонаблюдения за счет полного использования цифрового формата для отснятых изображений и высокопроизводительных компьютеров для цифровой обработки.

Совершенствование этой технологии, привело к развитию полуавтоматических систем, известных как второе поколение систем видеонаблюдения. Эти системы позволяют распознавать происходящие события на основе технологий машинного зрения. В настоящее время активно внедряются системы третьего поколения, основной отличительной чертой которых является иерархичность и распределенность информационных потоков. Таблица 1 иллюстрирует этапы технологического развития интеллектуальных систем видеонаблюдения.

Таблица 1

<i>Первое поколение</i>	
Технология	Аналоговые CCTV системы
Преимущества	– Хорошая производительность для простых задач – Проверенная временем технология
Проблемы	Аналоговые технологии для распространения и хранения данных
Текущее состояние	– Цифровое или аналоговое – Цифровая запись – Сжатие видео
<i>Второе поколение</i>	
Технология	Автоматическое видеонаблюдение с использованием технологий машинного зрения
Преимущества	Повышает эффективность систем CCTV
Проблемы	Требуются надежные алгоритмы
Текущее состояние	– Поиск надежных алгоритмов поведенческого анализа – Автоматическое обучение системы – Переход от статистического анализа сцены к пояснениям на естественном языке
<i>Третье поколение</i>	
Технология	Автоматическая система видеонаблюдения за большой территорией
Преимущества	– Более точная за счет применения различных датчиков – Распределенность
Проблемы	– Распределенность информации – Методология построения – Мультисенсорные платформы
Текущее состояние	– Распределенный или централизованный искусственный интеллект – Объединение информации – Система принятия решений на основе статистики – Многокамерные способы наблюдения

Типичными примерами коммерческих систем наблюдения являются DETEC [9] и Gotcha [9]. В их основе лежат датчики движения, также они могут сохранять в цифровом виде информацию об обнаруженных событиях (ключевых изображениях и метаданные с временными метками). Эти события, как правило, вызваны появлением новых объектов в сцене. DETEC основана на специальном оборудовании, которое позволяет подключить до 12 камер к одной рабочей станции. Рабочие станции могут быть подключены к сети и все данные наблюдения могут быть сохранены в центральной базе данных, доступной для всех рабочих станций в сети. Визуализация исходных изображений с камеры через Интернет описано в статье [10].

Еще одним примером коммерческой системы, предназначенной для применения вне зданий является DETER (Detection of Events for Threat Evaluation and Recognition) [9]. Она направлена на поиск необычных действий среди пешеходов и автомобилей в различных местах, например на парковках. Система состоит из двух частей: модуль компьютерного зрения и модуль оценки уровня угрозы. Первая часть занимается обнаружением, распознаванием и отслеживанием объектов. Для того, чтобы сделать это, система объединяет изображения со всех камер, а затем выполняет слежение за объектами. Оценка угрозы базируется на использовании высокоуровневых семантических методов, офлайн-обучения и онлайн-классификатора угроз. При работе на реальном объекте система показала хорошую производительность в распознавании объектов. Однако, как было указано в статье [10], DETER задействует относительно небольшое число камер, потому что каждая из них является достаточно дорогой. При этом эти системы не используют бихевиористический анализ.

В данной работе был предложен новый метод бихевиористического анализа поведения злоумышленников при помощи системы видеонаблюдения третьего поколения. Он заключается в фиксации и определении транспортных средств в нескольких наблюдаемых точках с дальнейшим анализом временных интервалов нахождения транспортных средств вне точек наблюдения.

2. Формализация задачи контроля над провозимыми грузами

Опишем систему провоза грузов более формально. Ключевые объекты:

- Завод/предприятие. Обладает обширной территорией, производит определенные товары. Через его территорию проходят различные транспортные средства.

- КПП. Поскольку в большинстве случаев территория завода ограничена неким защитным периметром, то есть так называемые КПП — контрольно-пропускные пункты. Весь автотранспорт и люди, желающие попасть (или покинуть) на территорию завода, должны пройти через один из таких пропускных пунктов. Обычно КПП оборудованы турникетами или шлагбаумами, которые управляются охранниками данного предприятия.
- Автотранспорт. Легковые и грузовые машины, проезжающие через территорию завода. Могут быть гружеными или пустыми.
- Система пропусков/накладных. На большинстве предприятий после загрузки машины продукцией, водителю выдаются определенные сопроводительные документы (обычно это товарная накладная), содержащие информацию о грузе (тип, вес), машине (марка, государственный номер) и водителе (ФИО, пропуск). Также, обычно есть отдельный пропуск на машину (временный или постоянный). Система накладных является частью системы электронного документооборота.

Что происходит с машиной:

1. Въезд на территорию завода. При этом проверяются документы водителя (основание для въезда), открывается шлагбаум КПП.
2. Машина въезжает на территорию завода.
3. Машина подъезжает к определенному цеху.
4. Проверка документов (оснований для выгрузки)
5. Происходит выгрузка продукции.
6. Машина подъезжает к другому цеху (или остается у того же).
7. Проверка документов (оснований для погрузки).
8. Происходит погрузка продукции.
9. Выдача сопроводительных документов.
10. Машина подъезжает к КПП.
11. Проверка сопроводительных документов.
12. Выезд машины с территории завода.

Очевидно, что шаги 4–5 и 6–9 — опциональны и не являются взаимоисключающими.

Рассмотрим теперь, на каких шагах наиболее вероятны попытки кражи.

Во-первых, возможен въезд нелегитимной машины на первом шаге. Например, с поддельным номером. Защита от этого одна — иметь реестр машин, допускаемых к въезду (с номерами и параметрами машины). При этом опять же есть угроза обмана со стороны охранников на КПП, если не ведется реестр всех их действий. Также в любом случае полезно фиксировать номера всех въезжающих машин.

Во-вторых, обман возможен на шаге номер три. Водитель может сгрузить часть продукции где-то на территории завода, например, спрятать ее. Притом, если:

- за машиной не проводится наблюдение,
- не проводится проверка качества и объема ввезенного товара,

то такой вариант кражи представляется весьма вероятным. Вариант защиты — отслеживать машину. Например, фиксировать ее проезд на определенных точках/дорогах завода и сравнивать с шаблоном стандартного проведенного времени (на нелегитимную выгрузку требуется достаточно много времени, плюс возможно отклонение от стандартного маршрута). То же самое возможно и после погрузки на 8 шаге, однако, водитель может проделать это и после выезда с завода, так что этот вариант воровства менее вероятен.

Еще один вариант — нелегитимный выезд, т. е. машина уже гружена нелегитимным товаром (без сопроводительных документов) и выезжает за счет «договоренности» с сотрудниками КПП. При отсутствии средств фактической фиксации проезда автомобиля, такая схема воровства весьма вероятна.

Как видно из вышеперечисленных примеров краж, без системы фиксации и/или контроля воровство предотвращать достаточно сложно. Перечислим теперь, какие технические средства позволяют сократить объемы воровства на предприятии.

- Система видеонаблюдения на КПП (только запись). Если система записывает все что происходит в режиме реального времени с камеры, расположенной на КПП, то при выявлении случая воровства, возможно отсмотреть весь объем видеоматериалов и выявить виновную машину. Минусы — много времени на просмотр, отсутствие системы оповещения, не спасает от воровства с помощью «зачачки». Плюсы — простота [2].
- Система видеонаблюдения на КПП с распознаванием номеров автомобилей. Это улучшенный вариант системы видеонаблюдения, который еще распознает номера всех машин, попадающих в обзор камер. Это позволяет вести список всего потока автомобилей, сравнивать его с неким разрешенным списком и легко (по номеру) искать все выезжающие машины в специальном реестре. Минусы — не предотвращает воровство с помощью «зачачки», возможны сбои в распознавании, повышенная сложность системы, отслеживает автомобили только в определенных точках. Плюсы — легкий поиск всех машин, возможность создания системы оповещения о событиях (например, о въезде машины с нелегитимным номером) [3].
- Распределенная система видеонаблюдения с распознаванием по всему заводу. Такая система имеет камеры не только на КПП, но и на дорогах на территории завода, во всех точках выгрузки и загрузки. Также система снимает содержимое кузова автомобилей, потенциально может опреде-

лять тип автомобиля — грузовой или легковой. Это позволяет отслеживать машину на пути всего ее следования по территории завода и выявлять нежелательное поведение. Например, если машина ехала несколько часов между двумя контрольными точками, то есть вероятность того, что водитель как раз делал «зачачку». Также если система получает информацию и грузе (через систему электронного документооборота), тогда возможно проверять и сам маршрут проезда (например, если в накладной заранее указан конечный цех). Также желательна ее интеграция с системами физического контроля — датчиками открытия-закрытия шлагбаумов, электронными весами для машин (чтобы проверить вес груза). Это позволит ей прозрачно и комплексно собирать информацию обо всех грузах, машинах, накладных, фактах открытия-закрытия шлагбаумов и т. д. Это позволит выявлять большую часть нелегитимных попыток вывезти товар. Минусы — большая сложность системы, большое количество камер. Плюсы — полный и прозрачный контроль над всеми грузами и автомобилями проходящими через территорию завода [4]. Отметим, что система — не человек и «дать ей взятку» — не получится. Также можно дополнить ее определенными системами, защищающими ее от попыток взлома — например, в случае кражи камеры или обрезки проводов, система начинает бить тревогу, вплоть до блокировки всех КПП — до получения специального разрешения от руководства, система физически блокирует выезд всего автотранспорта с завода.

Последний вариант, несмотря на высокую стоимость и определенную техническую сложность является наиболее подходящим для организации системы комплексной безопасности, поскольку:

- Минимально участие человека. Все события — выезд, въезд, погрузка фиксируются. Притом возможно создавать фотографии не только самой машины, но и содержимого кузова, для последующей проверки экспертом, в случае подозрений.
- Интеграция с системой электронного документооборота. Это позволяет фиксировать в системе дополнительные сведения о грузе, машине и водителе. А также отправлять в систему фактические данные:
 - данные датчиков открытия-закрытия шлагбаумов,
 - данные о распознанных номерах,
 - данные о фактическом проезде автомобиля.
- Шаблоны нормального поведения машин. Становится возможным полностью отслеживать маршрут движения машины, а также время прохождения контрольных точек. При этом возможно

выявлять отклонения, например: нелегитимный маршрут, подозрительное время следования.

- Система объективного контроля. Например, система распознает номер выезжающей машины и сравнивает его с указанным в электронной накладной. В случае несоответствия — фиксируется попытка нелегитимного вывоза. Обмануть такую систему — достаточно сложно. Подмена и заклейка номера после въезда — исключаются, поскольку за машиной проводится постоянное слежение на всей территории завода.

Таким образом, мы видим, что система исключает множество (хотя и не все) возможных вариантов хищения. Притом в любом случае остается большая доказательная база — видеоматериалы, данные системы распознавания и т. д., которые окажут значительную поддержку в случае расследования любого инцидента.

Примером такой системы является система «Цербер» — модульная комплексная система видеонаблюдения и распознавания.

3. Цели создания системы «Цербер»

Цели создания системы «Цербер»:

- Снизить объем хищений на площадках завода. Ожидаемая цифра снижения объема хищений — 50–60 %.
 - Получить контроль и статистику по автотранспорту, въезжающему и выезжающему с территории заводов, а именно:
 - список всех автомобилей проехавших по территории завода,
 - маршрут каждого автомобиля, проехавшего через территорию завода,
 - статистика по каждому водителю, цели — среднее время на маршруте, среднее время проведенное на территории завода,
 - список «аномалий» — слишком долгих или коротких маршрутов.
 - Получить резервную систему видеонаблюдения. С привязкой к реестру распознанных номеров, для того чтобы облегчить поиск отдельной машины.
 - Оценить эффективность работы водителей транспортных средств.
- Решаемые системой задачи:
- Регистрация номеров и фотофиксация автомобилей, въезжающих на территорию, выезжающих с территории и перемещающихся через ключевые точки территории ИМЗ. При этом возможно фиксировать при помощи видеокamer груз, находящийся в кузове машины, и наблюдать за изменением содержимого кузова на территории заводов.

- Построение пути следования автомобилей (включая затраченное на каждый участок время), анализ соответствия фактического пути одному из заранее определенных (эталонному), оповещение о подозрительном поведении. Следует отметить, что это также позволит оценивать эффективность работы водителей.
- Интеграция с системой электронного документооборота и отделом пропусков: извлечение данных о предполагаемом маршруте, о допуске машины на территорию, времени начала и конца действия пропуска; экспорт данных о фактическом пути следования транспортных средств, на которые был оформлен пропуск.
- Организация системы видеонаблюдения и ведение видеоархива с использованием рабочих и дополнительных телекамер в целях резервирования системы «Videonet».

4. Архитектура системы «Цербер»

Комплекс видеоконтроля имеет структуру, описанную ниже.

1. **Точки контроля** — набор телекамер, наблюдающих за одним каким-либо направлением проезда определенной точки.
2. **Посты** — пункты сбора данных с одной или нескольких точек контроля, объединяющие.
3. **Центр сбора данных** — место объединения и хранения данных о движении транспорта с постов контроля.
4. **Центр ведения видеоархива**, — место объединения и хранения видеоданных с постов контроля.

Связь между точками контроля и постами осуществляется посредством проложенных коаксиальных, оптоволоконных, витой пары и силовых кабелей, а между постами и центрами системы — посредством имеющейся на предприятии сетевой инфраструктуры.

Пользователи работают с системой посредством рабочих компьютеров, также подключенных к сети предприятия посредством веб-браузера. Это избавляет от необходимости использования стороннего программного обеспечения.

Экспорт данных в систему электронного документооборота организуется посредством взаимодействия с ПО «Цербер-Сервер» по согласованным спецификациям. По сути это связь с электронной системой документооборота, являющаяся двусторонней — системе передаются данные о фактах проезда определенных автомобилей/поездов в виде XML файла, созданного по предварительно заданному шаблону. Также система в форме того же XML передает данные из электронных накладных для автомобилей.

Распределенность системы — один из ее основных плюсов, позволяющий снизить нагрузку на центральный сервер, а также повысить надежность и масштабируемость системы. Также это позволяет гибко добавлять новые модули и датчики в уже существующую систему. Единицей системы является пост — к нему подключены камеры системы, а также различные датчики. Серверная часть не имеет ограничений на количество одновременно подключенных постов.

Одной из основных потенциальных проблем является ломка и порча оборудования, поэтому все камеры, ЭВМ и другие части системы ставятся в максимально защищенных и неудобных для воров местах. Также все камеры прокладываются под землей в защищенных трубах, чтобы избежать кражи кабелей.

5. Схема работы системы

Распишем по шагам схему работы системы.

1. Машина подъезжает к КПП и останавливается у шлагбаума.
2. Индуктивный датчик фиксирует факт подъезда машины к КПП и сообщает об этом компьютеру на посту.
3. Программная часть комплекса «Цербер» фиксирует наличие автомобиля в видеопотоке.
 - a. Происходит распознавание номера.
 - b. Фиксируется факт открытия шлагбаума.
 - c. В базу данных заносится запись о въезде автомобиля на территорию предприятия.
 - d. В видеоархив пересылаются фотографии и видеофрагмент въезда автомобиля с временными метками.
 - e. Из системы электронного документооборота извлекаются данные о целях въезда — цеха, которые должен посетить данный автомобиль.
 - f. Система начинает слежение за автомобилем.
4. Машина въезжает на территорию завода.
5. Машина следует по территории завода.
6. На всех регистрирующих постах по пути следования автомобиля, фиксируется его проезд.
 - a. Индуктивный датчик фиксирует факт подъезда машины к КПП и сообщает об этом компьютеру на посту.
 - b. Происходит распознавание номера.
 - c. Данные о проезде автомобиля пересылаются в базу данных.
 - d. В видеоархив пересылаются фотографии автомобиля с временными метками.
 - e. Происходит проверка легитимности маршрута следования (описана ниже).
 - f. В случае выявления отклонений данные пересылаются в Единый центр, происходит оповещение о подозрительном событии.

7. На всех регистрирующих постах в цехах по пути следования автомобиля, фиксируется его проезд.
 - a. Индуктивный датчик фиксирует факт подъезда машины к цеху и сообщает об этом компьютеру на посту.
 - b. Данные о проезде автомобиля пересылаются в базу данных.
 - c. В видеоархив пересылаются фотографии автомобиля с временными метками. Также обязательно создается и пересылается фотография содержимого кузова автомобиля.
 - d. Происходит проверка легитимности маршрута следования (описана ниже).
 - e. В случае выявления отклонений данные пересылаются в Единый центр, происходит оповещение о подозрительном событии.
8. Машина выезжает с территории завода.
9. Программная часть комплекса «Цербер» фиксирует наличие автомобиля в видеопотоке на выезд.
 - a. Индуктивный датчик фиксирует факт подъезда машины к цеху и сообщает об этом компьютеру на посту.
 - b. Данные о проезде автомобиля пересылаются в базу данных.
 - c. В видеоархив пересылаются фотографии автомобиля с временными метками
 - d. Из системы электронного документооборота берутся данные о номере этой машины.
 - e. Происходит сверка номера в накладной с номером выезжающей машины.
 - f. В случае несовпадения номеров, выезд блокируется высылается оповещение о подозрительном событии. В противном случае — переход на шаг *h*.
 - g. Оповещается охранная компания.
 - h. Блокировка снимается сотрудниками охранной компании, система переходит в нормальный режим работы.
 - i. В случае выявления отклонений данные пересылаются в Единый центр, происходит оповещение о подозрительном событии.

6. Алгоритм распознавания номеров

С точки зрения программного обеспечения, распознавание номеров в общем виде представляет совокупность алгоритмических этапов:

1. Этап обнаружения движения: представляет собой программный механизм, анализирующий кадры, поступающие с видеокамеры. Также о присутствии движения могут уведомлять внешние устройства (специальные датчики, предназначение для слежения за движением в контролируемой зоне (например, инфракрасные датчики движения)).

Данный этап необходим для отсеивания неинформативных изображений, на которых нет движения и, скорее всего, нет машины с номером.

2. Локализация (выделение) областей изображения (зон), в которых потенциально содержатся номера машин, приведение различных параметров зон к однотипному виду (например, изменение размеров). При этом используются стандартные методики.
3. Формирование набора признаков изображения, содержащих данные о яркостных характеристиках, форме и изгибам символа и другие важные параметры.
4. Отнесение образа на изображении к одному из известных классов на основании сформированных признаков. Это фактически и есть распознавание.
5. Этап принятия решения: аккумулирует информацию о распознанных номерах на нескольких изображениях и формирует одно итоговое решение.

За исключением третьего и четвертого этапов, все шаги являются достаточно тривиальными и не представляют научного интереса. Основной проблемой является именно выделение ключевых признаков и само распознавание. Для распознавания автомобильных номеров было решено использовать так называемый тестовый алгоритм, относящийся к классу алгоритмов частичной прецедентности. Теоретическая база алгоритмов частичной прецедентности (вычисления оценок, голосования, или комбинаторно-логических алгоритмов) описана в научных публикациях [5–7], и другие.

Принципиальная идея данных алгоритмов основана на отнесении распознаваемого объекта S в тот класс, в котором имеется большее число «информативных» фрагментов эталонных объектов («частичных прецедентов»), приблизительно равных соответствующим фрагментам объекта S . Вычисляются близости — «голоса» (равные 1 или 0) распознаваемого объекта к эталонам определенного класса по разным информативным фрагментам объектов данного класса. Данные близости суммируются и нормируются на число эталонов этого класса. В результате вычисляется нормированное число голосов, или оценка объекта S за класс $\Gamma_j(S)$ — эвристическая степень близости объекта S к классу K_j . После вычисления оценок объекта за каждый из классов, осуществляется отнесение объекта к одному из классов с помощью порогового решающего правила. Подробное описание алгоритма можно найти в [6].

На практике это означает, что в силу стандартности формы автомобильных номеров, после шага два, номер разбивается на стандартные участки, в каждом из которых при помощи тестового алгоритма происходит попытка распознавания цифры/буквы.

Каждая буква/цифра при этом задается бинарной матрицей 16×16 .

По результатам тестирования средняя точность распознавания — около 90–95 % для выборки из 1500 номеров.

7. Алгоритм проверки легитимности действий водителя

Представим территорию завода и всего его дороги в виде связного графа $G=(V,E)$, где вершины инцидентности 1 — Контрольно-пропускные пункты на въезд-выезд.

Автомобиль следует по маршруту, который теперь можно представить в виде пути в графе (v_1, \dots, v_n) , при этом инцидентность вершин v_1, v_n равна единице.

Также есть база временных интервалов следования автомобиля между вершинами графа v_i, v_{i+1} — $t'_{i,i+1}$. В таком случае если обозначить фактическое время следования автомобиля за $t_{i,i+1}$, тогда погрешность следования на i участке маршрута:

$$t_{i,i+1} - t'_{i,i+1}.$$

Если эта разность составляет более 20 минут — это подозрительная задержка движения. Назовем это критерием нарушения первого рода.

Далее, по достижении конечной точки следования v_n производится подсчет суммарного отклонения:

$$\sum_{i=1}^n (t_{i,i+1} - t'_{i,i+1}).$$

Если эта разность составляет более 20 минут — это подозрительная задержка движения. Назовем это выражение критерием нарушения второго рода.

Теперь опишем то, каким образом рассчитывается среднее время движения на каждом интервале. Во-первых, все автомобили разделяются на грузовые и легковые — скорость грузовых очевидно ниже, плюс они проходят более тщательный досмотр на точках КПП. Обозначим среднюю скорость легковых как l , а грузовых как m . Среднее время досмотра автомобиля на КПП — c .

Далее, для каждого участка v_i, v_{i+1} известно его расстояние, измеренное в метрах — $d_{i,i+1}$. Тогда, для каждого участка v_i, v_{i+1} , если инцидентность v_{i+1} всех вершин, инцидентности более 1 среднее время допустимого проезда легковой машины:

$$t'_{i,i+1} = \frac{d_{i,i+1}}{l},$$

грузовой машины:

$$t'_{i,i+1} = \frac{d_{i,i+1}}{m}.$$

В случае же проезда к КПП необходимо добавить время на досмотр грузового автомобиля:

$$t'_{i,i+1} = \frac{d_{i,i+1}}{m} + c.$$

Заключение

В работе была формально описана и предложена система комплексного видеонаблюдения за автотранспортом на предприятии. Были описаны требования к таким системам, достоинства и недостатки различных подходов к построению таких систем.

Была предложена и описана система комплексного видеонаблюдения Цербер, которая позволяет:

- Регистрировать номера автомобилей, въезжающих на территорию, выезжающих с территории и перемещающихся через ключевые точки территории предприятия.
- Строить пути следования автомобилей (включая затраченное на каждый участок время), анализ соответствия фактического пути одному из заранее определенных (эталонному), оповещение о подозрительном поведении.
- Обмениваться данными с системой электронного документооборота и отделом пропусков.
- Вести видеоархив.

Абрамов Николай Александрович. Аспирант ВЦ РАН. Окончил МГУ им. М. В. Ломоносова в 2010 г. Количество печатных работ: 7. Область научных интересов: информационная безопасность, безопасность промышленных объектов, оптимальное управление. E-mail: cunick@gmail.com

Литература

1. Сборник статистических сведений ГИЦ МВД России за 2003 г. Ф1А. Кн. 81. Т. 2.
2. *Ferryman J. M., Maybank S. J., and Worrall A. D.* Visual surveillance for moving vehicles // *International Journal of Computer Vision*, 37(2): 187–143, Kluwer Academic Publishers, Netherlands, 2000.
3. *Jaynes C.* Multi-view calibration from planar motion for video surveillance. In *Second IEEE International Workshop on Visual Surveillance*, Colorado, 1999, pp. 2–67, ISBN 0–7695–0037–4.
4. *Garcia L. M. and Grupen R. A.* Towards a real-time framework for visual monitoring tasks. In *Third IEEE International Workshop*.
5. *Журавлев Ю. И.* Избранные научные труды. М.: Издательство «Магистр», 1998. 420 с.
6. *Журавлев Ю. И.* Об алгебраическом подходе к решению задач распознавания или классификации // *Проблемы кибернетики*. М.: Наука, 1978. Вып. 33. С. 5–68.
7. *Журавлев Ю. И., Никифоров В. В.* Алгоритмы распознавания, основанные на вычислении оценок // *Кибернетика*. 1971. № 3. С. 1–11.
8. *Paulidis I. and Morellas V.* Two examples of indoor and outdoor surveillance systems. In *Video-Based Surveillance Systems*, P. Remagnino, G. A. Jones, N. Paragios, and C. S. Regazzoni, Eds. Kluwer Academic Publishers, Boston, 2002, pp. 39–51.
9. *Pavlidis I., Morellas V., Tsiamyrtzis P., and Harp S.* Urban surveillance systems: from the laboratory to the commercial world. In *Proceedings of the IEEE*, 2001; 89(10): 1478–1495.