МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

АЛМАТИНСКАЯ АКАДЕМИЯ
ИМЕНИ МАКАНА ЕСБУЛАТОВА

ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ВИДЕОАНАЛИТИКИ, В ТОМ ЧИСЛЕ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ХОДЕ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ

Методические рекомендации

Алматы, 2024

Методические рекомендации обсуждены и одобрены на научно-методическом заседании Алматинской академии МВД Республики Казахстан им. М. Есбулатова. Протокол №7 от «19» сентября 2024г.

Рецензенты:

Коржумбаева Т.М. – начальник кафедры административно-правовых дисциплин Алматинской академии МВД Республики Казахстан им. Макана Есбулатова, к.ю.н., ассоциированный профессор (доцент), полковник полиции

Аубакирова А.А. – профессор кафедры права, общей и социальной психологии Алматинского филиала Санкт-Петербургского гуманитарного Университета профсоюзов, д.ю.н, профессор

Стамбеков О.Е., Кудайбергенов Е.Б., Сарсенбаева Б.Б. Правовые основы использования системы видеоаналитики, в том числе с применением искусственного интеллекта в ходе расследования уголовных дел: Методические рекомендации – Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан им. М. Есбулатова, 2024. – 56 с.

Методические рекомендации подготовлены в соответствии с Планом НИД Алматинской академии позиция 7 – «Правовые основы использования системы видеоаналитики, в том числе с применением искусственного интеллекта в ходе расследования уголовных дел» (2024г.), и разработаны с учетом современных требований криминалистики, уголовного и уголовно-процессуального законодательства. Отражают основные понятия, стандарты видеоаналитики.

Методические рекомендации предназначены для сотрудников правоохранительных органов, а также научных и практических работников системы ОВД, преподавателей и обучающихся ведомственных и иных юридических учебных заведений.

Введение

Вы когда-нибудь задумывались, что происходит с записями с камер видеонаблюдения?

Записи видеонаблюдения являются важным инструментом в руках следователей по уголовным делам.

В случае совершения преступления или подозрения, что преступление будет совершено, правоохранительные органы используют все улики, включая записи камер наблюдения для установления личности преступников, проводится анализ записей видеонаблюдения для установления, устранения или предотвращения угрозы.

До появления видеоаналитики, основную работу приходилось выполнять людям. Необходимо было просмотреть многочасовые видеоданные, оценить любую связанную с ними информацию с последующим установлением факта преступления. Это был утомительным и громоздким процесс, с проблемами, возникших из-за человеческих ошибок.

Учитывая, что наблюдение ведется круглосуточно. Существует необходимость исключить вмешательство человека при обработке данных наблюдения. Видиоаналитика быстрее и эффективней выполнять работу по оценке данных и тщательному анализу исторических данных, записанных за определенный период времени.

Эффективность компьютерной видеоаналитики

Применение видеоаналитики в системе распознавания преступников в правоохранительной деятельности имеет ряд эффективных преимуществ:

1. Повышение точности и скорости идентификации.
2. Обработка большого объема данных.
3. Непрерывность мониторинга.
4. Объективность и беспристрастность.
5. Возможность автоматического реагирования

Таким образом, применение видеоаналитики значительно повысит эффективность работы правоохранительных органов в вопросах распознавания и поиска преступников.

Современное состояние видеоаналитики с применением искусственного интеллекта

Видеоаналитика – это технология, использующая методы компьютерного зрения для автоматизированного получения различных данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей.

В основе программного обеспечения лежит комплекс алгоритмов позволяющих вести видеомониторинг и производить анализ данных без прямого участия человека.

Функции видеоаналитики строятся по схеме: камера + back-end аналитика. Т.е. камера гонит поток видео на сервер, а специальное ПО на сервере уж делает весь видеоанализ.

Видеоаналитика позволяет гибко управлять видеопотоками при анализе их контента «на лету», при автоматизации аналитических функций.

Это позволяет сотруднику концентрироваться на определённых инцидентах на видеозаписи, системы видеоаналитики могут начинать запись, только при начале какого-то движения в зоне обзора камеры. При этом снижается нагрузка на сеть и экономится пространство в системе хранения.

Интенсивность использования функций видеоаналитики можно гибко регулировать по мере потребностей, выбирая именно те функции, которые нужны в конкретном случае. Это позволяет создавать кастомизированные решения.

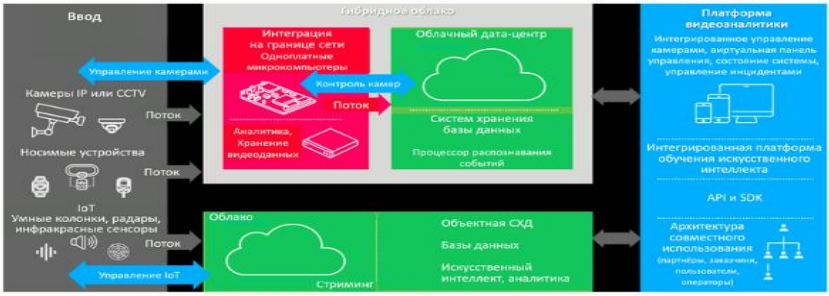


Рис. Типовая системная архитектура видеоаналитики

Видеоаналитика – это приложения компьютерного зрения, которые извлекают информацию и знания из видеоконтента, то есть дают ответы на вопросы: (Кто: распознавание и идентификация людей, Что: объекты, действия, события, поведение, взаимоотношения; Где: геолокация, пространственная (3D) и планарная (2D) локация, Когда: маркировка даты и времени, сезона).

Типы приложений видеоаналитики:

1. Ретроспектива: управление архивами видеозаписей, поиск, сортировка, получение юридических доказательств;

2. Настоящий момент: что происходит сейчас, контроль ситуации, получение предупреждений в реальном времени, кодирование, компрессия видеопотока;

3. Взгляд в будущее: предсказания на основе событий прошлого и настоящего, прогнозирование событий или активности, детектирование аномалий.

Типы платформ видеоаналитики:

1. Видеоаналитика на выделенном сервере (сервер интеллектуального видеонаблюдения IVS (Intelligent Video Surveillance) и сервер автоматического распознавания номеров автомашин ALPR (Automatic License Plate Recognition). Они хорошо масштабируется при увеличении числа камер и *позволяет ввод новых функции анализа* видеоизображений.

2. Видеоаналитика на сетевом видеорекордере NVR (Network Video Recorder, обладает некоторыми встроенным функциями видеоаналитики. Ввод новых аналитических функций в этом случае *либо невозможен, либо сложен*.

3.Видеоаналитика на камерах (Камеры видеонаблюдения обладают встроенными функциями видеоаналитики. Преимуществом является то, что возможности аналитики в таких камерах не зависят от полосы пропускания сети и времени отклика сервера. Такое решение выгодно там, где требуется *высокая оперативность и немедленный отклик.*

Анализ больших данных, искусственный интеллект

Технологии Искусственного Интеллекта (ИИ) быстро и широко применяются в видеоаналитике. По сути они являются нейросетью с возможностью обучения.

Существует три основных метода обучения нейросетей:

– При обучении с учителем нейронная сеть обучается на предварительно размеченном наборе данных для получения ответов, которые используются для оценки точности алгоритма на обучающих данных.

– При обучении без учителя модель использует неразмеченные данные, из которых алгоритм самостоятельно пытается извлечь признаки и зависимости.

– Обучение с частичным привлечением учителя, использует небольшое количество размеченных данных и большой набор неразмеченных данных.

– Обучение с подкреплением тренирует алгоритм при помощи системы поощрений.

Поэтому, когда мы говорим об использовании ИИ в видеонаблюдении, мы фактически имеем в виду использование нейросетей с возможностью обучения без учителя.

Использование ИИ в видеонаблюдении

В университете Карнеги (США) в 2019 году было проведено исследование использования ИИ для видеонаблюдения и был разработан Глобальный Индекс использования ИИ для видеонаблюдения AIGS (AI Global Surveillance), который показывает степень использования ИИ для видеонаблюдения в 176 странах мира (без различия легитимности такого использования).

Наиболее часто ИИ используется в таких приложениях видеоаналитики, как платформы Умного или Безопасного Города (56 стран), системах распознавания лиц (64 страны), а также в системах Умной охраны правопорядка, Smart Police (52 страны).

Стандарты видеоаналитики

Ситуационная видеоаналитика. «Термины и определения» должны является первыми в группе стандартов, устанавливающих нормативные требования в области ситуационной видеоаналитики, регламентирующие эксплуатационные характеристики, методики испытаний и оценки качества и требования к размещению оборудования технических систем интеллектуального видеонаблюдения.

Принятие стандарта позволит упорядочить нормативное регулирование в области ситуационной видеоаналитики и устранить технические барьеры при ее применении.

Современные системы видеонаблюдения применяют интеллектуальные технологии обработки данных, позволяющих в реальном времени анализировать не только отдельные изображения, но и целые последовательности динамических событий и сцен.

Отсутствие терминологического единства в этой области зачастую ставит заказчиков и интеграторов систем в сложное положение, затрудняя выбор решения, оптимального в каждом конкретном случае

Функциональные возможности

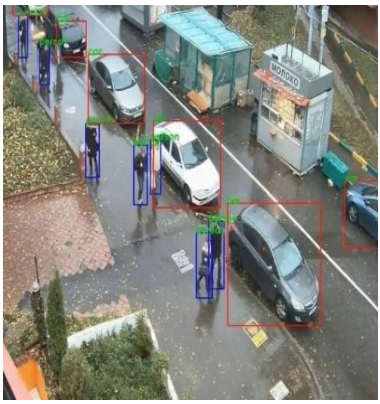
1. Улучшение изображений

– алгоритмы восстановления и улучшения изображений, такие как шумоподавление.

– устранение размытости.

– методы повышения чёткости изображений при помощи нейросетей: «супер-разрешение» на базе нескольких изображений объекта.

– супер-разрешение на базе единственного изображения.



2. ***Детектирование движения*** – процесс обнаружения изменения положения объекта относительно его окружения или изменения окружения относительно объекта. При сравнении нескольких последовательных изображений сцены, система видеоаналитики может распознать начало движения какого-либо объекта внутри сцены.

3. **Распознавание лиц** – практическое приложение в задачу которого входит автоматическая локализация лица на неподвижном или движущемся изображении и, в случае необходимости, идентификация личности по характерным параметрам лица. (Определение личности человека по расстоянию между характерными точкам).

4. **Распознавание бесцельного поведения**

– это нахождение на одном месте или в пределах одной сцены в публичном пространстве в течение продолжительного времени без определённой цели. (*белая пунктирная линия*).

5. Распознавание пропажи, либо оставленных без присмотра объектов

Такие объекты в системах видеоаналитики обычно выделяются рамками с соответствующим пояснением. Это может быть признаком готовящегося преступления, поэтому на основе данных видеоаналитики необходимо как можно быстрее задержать подозрительного субъекта, оставившего предмет, и выяснить, что именно он оставил в нём.

Аналогично может распознаваться пропажа (исчезновение) объекта. В этом случае система видеоаналитики немедленно выдаёт предупреждение тем или иным образом.

6. Закрытая зона

При проникновении людей в закрытую зону система выдаёт предупреждение, выделяя нарушителя рамкой.

7. Детектирование проникновения

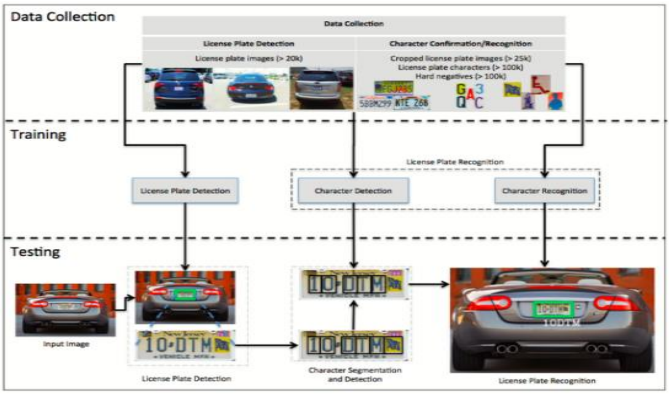
Детектирование проникновения – часть сервиса «Закрытая зона».

8. Распознавание автомобильных номеров

Автоматическое распознавание номерных знаков — это технология видеоаналитики, которая использует оптическое распознавание символов на изображениях для считывания регистрационных знаков транспортных средств для получения информации о местонахождении транспортных средств.

Процесс распознавания номера автомобиля, состоит из трёх стадий:

1. Обнаружение номера, обнаружение символов на номере.
2. Процесс обучения
3. Распознавание символов, при котором используются методы машинного обучения системы видеоаналитики.



9. Слежение за объектами

Слежение за объектами – вспомогательный сервис для услуги распознавания «бесцельного поведения», он может использоваться и для иных целей, система видеоаналитики

обучена производить распознавание такого поведения субъектов, с выдачей предупреждения о подозрительном поведении.

Интеграция функций

Многие функции видеоаналитики часто представляют собой интеграцию нескольких базовых функций.

– Проникновение в закрытую зону;

– Оставление объектов без присмотра в течение определённого времени;

– Распознавание движения объектов;

– Распознавание номеров.

Подсчёт людей и транспорта

1) Системы подсчёта также могут анализировать маршруты и поведение людей.

2) Количество машин, проезжающих по улице за определённый промежуток времени, в зависимости от времени суток, дня недели и сезона;

3) Количество машин, скапливающихся у светофора и среднее время ожидания проезда перекрёстка;

4) Количество машин, проезжающих через КПП в закрытую зону и выезжающих из неё;

5) Заполняемость уличных парковок и её зависимость от времени;

6) А также другую информацию.

По собранной информации можно рассчитать такие показатели как:

1) средняя скорость потока;
2) объем потока (количество транспортных средств в час);
3) плотность потока;
4) средняя занятость полосы;
5) длина транспортных средств (для решения задачи классификации транспортных средств);
6) длина очереди перед перекрёстком;
7) детектирование выезда на встречную полосу.

10. Анализ видеонаблюдения ограниченной зоны и периметра

Аналитика систем видеонаблюдения для охраны закрытых зон и периметров предназначена для выявления попыток несанкционированного проникновения в закрытую зону, даже в отсутствие физического ограждения.

1) поиск, обнаружение и распознавание подозрительных предметов и людей;

2) выявление и распознавание изменений видеоизображений определённых зон во времени.

3) выявление потенциальных угроз;

4) определение вероятностей реализации потенциальных угроз;

5) определение уязвимых зон;

6) обнаружение факта пересечения периметра;

7) информирование о потенциальных угрозах или фактах проникновения;

8) рассылка извещений и изображений инцидента.

Распознавание лиц

Для распознавания лиц подойдёт любая система видеонаблюдения с разрешением не менее Full-HD, со встроенной функцией распознавания лиц, что позволит создавать базы данных и автоматически отправлять уведомления с предупреждением.

Основные шаги процесса распознавания лиц:

1. Из фото-картинки или видеозаписи извлекается изображение лица (детекция лица). Лицо может быть как одиноким, так и находится в окружении многих лиц. Поворот головы не оказывает решающего влияния на этом шаге.

2. Приложение распознавания лиц может считывать геометрические параметры лица: такие как расстояние между глазами, расстояние от лба до подбородка и др. Всего могут учитываться до 100 и более подобных геометрических параметров. На основе этих данных составляется цифровая сигнатура лица.

3. Сигнатура лица сравнивается с другими сигнатурами из базы данных физических лиц используемых сотрудниками ОВД.

4. Определение личности человека должна быть с достаточно высокой точностью, превышающей 90%.

Практическое применений распознавания лиц при помощи видеоаналитики:

1. Безопасность в аэропортах, для определения, людей с просроченной визой или находящихся в розыске, лиц находящихся под подпиской или под другими мерами пресечения по уголовным делам.

2. Контроль на экзаменах в учебных заведениях. Это является эффективным средством против попыток сдачи экзаменов подставными лицами вместо неуспевающих студентов.

3. Социальные веб-медиа. Facebook использует алгоритм для нахождения лиц при загрузке фото на платформу, при этом выдаётся запрос, хотите ли вы отметить друзей на фото. При утвердительном ответе на вопрос, создаётся линк на страницы отмеченных друзей. Точность распознавания лиц на Facebook составляет 98%.

4. В Религиозных сообществах, для контроля тех, кто регулярно ходит на службы, чтобы отслеживать активность верующих, а также вносящих пожертвования.

5. В торговых центрах, для распознавания подозрительных лиц и выявления потенциальных нарушителей.

Сервер системы видеоаналитики воспринимает сигналы предупреждения от программы видеоаналитики, которая работает со множеством видеокамер, установленных на территории.

Возможные действия реакции на предупреждающие сигналы:

– Управление камерами (движение, запись и пр.);

– Предоставление новой видео- и аудиоинформации для операторов и сотрудника, например, изменение точки обзора, включение дополнительных микрофонов;

– Команды для других подключённых устройств или программ через протокол HTTP

– Команды через интерфейс пользователя (Windows) для запуска и настройки других устройств или ПО;

– Запуск SNMP-ловушек для индикации состояние ПО мониторинга под управлением протокола SNMP;

– Журналирование предупреждающих сообщений и сохранение их в базах данных для последующего анализа.

Обеспечение безопасности

Видеонаблюдение – основное средство предотвращения и расследование случаев воровства, несанкционированного проникновения, вандализма, терроризма и других нежелательных действий.

Важной частью системы видеоаналитики является способность проактивно извещать сотрудников правоохранительных органов, для быстрого реагирования, и предотвращения преступлений и возникновения ущерба.

На дорогах системы видеонаблюдения с функцией распознавания автомобильных номеров выполняют следующие основные задачи:

1) Контроль правил дорожного движения (ПДД)

Автоматическое выявление нарушений, таких как: превышение скорости, проезд на красный свет, движение по запрещённым полосам или нарушение разметки. А также для формирования доказательной базы.

2) Мониторинг транспортного потока

Системы фиксируют номерные знаки автомобилей для подсчёта транспортного потока и анализа загруженности дорог.

Помогают в организации движения и оптимизации дорожной инфраструктуры.

3) Распознавание и поиск транспортных средств

Выявление автомобилей, находящихся в розыске (например, угнанных или используемых в противоправной деятельности). Использование черных и белых списков для выделения автомобилей, требующих особого внимания.

4) Обеспечение безопасности

Сопровождение транспорта на пограничных переходах, КПП и других стратегических объектах. Предупреждение попыток использования подложных номерных знаков.

5) Автоматизация процессов

Функции интеграции с платными дорогами для расчёта стоимости проезда на основе номера транспортного средства.

Упрощение управления въездом/выездом, например, для парковок.

Поиск и отслеживание подозрительных лиц

При выборе подозрительного персонажа на записи с камеры, видеоаналитика может выполнить следующие действия:

– Сделать стоп-кадр и создать видеоклип с изображениями похожих людей на записях с других камер в хронологическом порядке;

– Построить траекторию движения объекта.

Возможен поиск объектов в видеоархиве с использованием загруженных изображений в соответствии со следующими параметрами:

– Форма; Цвет; Размер;

– Положение в кадре.

Трекинг объектов (основные функции):

– перемещения объекта наблюдения;

– немедленное извещение тревоги;

– пересечение объектом заданной линии;

– Перемещение объекта по заданной зоне;

– Долгое нахождение объекта на одном месте.

– Предотвращение возможных террористических атак.

Функции видеоаналитики позволяют предотвратить следующие виды саботажа:

– Расфокусировка видеокамеры;

– Поворот камеры в сторону от установленного для неё направления съёмки;

– Длительное ослепление камеры;
– Перегораживание вида камеры.

Развёртывание изображения с панорамной камеры типа «рыбий глаз»

Возможно получение «плоского» изображения с панорамной камеры типа «рыбий глаз», которая обычно сильно искажает перспективу изображения. При этом становится возможным заменить несколько обычных камер на одну панорамную с более широким функционалом, и контролировать несколько зон при помощи одной камеры.

В современных системах видеоаналитики могут использоваться интеллектуальные камеры со встроенной обработкой видео или специальные аналитические программные платформы, работающие на удалённом сервере.

В таких платформах всё чаще используются алгоритмы *машинного обучения*, чтобы облегчить интерпретацию и анализ данных во всё более увеличивающихся объёмах потоков видео-контента.

Использование нейросетей и глубокого обучения

Использование высокоточных нейросетей в видеоаналитике позволяет значительно расширить функционал.

Нейросети широко используются для точного и достоверного *распознавания изображений.*

Интеллектуальное видеонаблюдение в «умном городе»: контроль и защита визуальных персональных данных

Видеонаблюдение со встроенной видеоаналитикой, позволяют осуществлять мониторинг безопасности на определенной местности с оперативным реагированием.

Автоматизированная система, основанная на анализе потоков данных от различных источников информации, которая позволяет производить обработку полученных сведений в реальном времени, осуществлять многофакторный анализ и инициировать оперативное реагирование как в режиме

поддержки принятия решений с участием человека, так и в полностью автоматическом режиме.

Видеоаналитика включает в себя обнаружение и распознавание людей, сопровождение их перемещения на видео, повторную идентификацию (реидентификацию) людей в мультикамерных системах видеонаблюдения, определение нехарактерного поведения людей.

При использовании видеоаналитики должен соблюдаться баланс интересов человека и государства.

– С технической стороны должна быть обеспечена безопасность и непрерывность функционирования таких систем.

– С правовой стороны: человек должен иметь возможность защищать свое право на неприкосновенность частной жизни.

– Необходимо создать республиканскую систему мониторинга безопасности» (далее – РСМБ) которая по единым техническим стандартам, будет повышать уровень безопасности

Система должна объединять на одной платформе:

1. локальные системы видеонаблюдения
2. специальные детекторы
3. каналы связи
4. центр обработки данных
5. иные системы и информационные ресурсы.

При этом обработка и хранение информации в системе мониторинга должна осуществляться посредством программной платформы и аппаратного комплекса центра обработки данных.

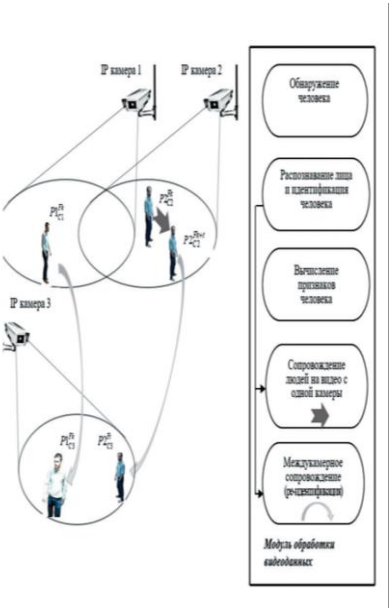
При практической реализации алгоритмов обработки видео

– на первом шаге должно выполнятся обнаружение объектов и их локализация или же детектирование областей-кандидатов, которые могут быть отнесены к объектам интереса

– следующий этап требует вычисления признаков выделенных фрагментов (лица), на основе которых выполняется анализ и конечная их классификация.

Видеонаблюдение с функциями обнаружения, идентификации, отслеживания и реидентификации людей

Система видеонаблюдения должна состоять из территориально разнесенных IP-камер и организована на основе единого центра обработки данных.



Упрощенная структура пространственно-распределенной видеосистемы с функциями обнаружения и отслеживания людей для трех IP-камер.

С помощью детектора выполняются обнаружение всех людей, попадающих в поле зрения камер, формирование ограничительных рамок, которые описывают прямоугольником обнаруженные фигуры для них. Эти изображения людей размещаются в галерее, и для каждого из них с помощью ***сверточных нейронных сетей (далее – СНС)*** определяются векторы СНС-признаков (СНС-дескрипторы), формирующие общее пространство СНС-признаков, которое представляется в виде таблицы, где каждая строка является СНС-дескриптором для одного изображения. В каждой обнаруженной области выполняется поиск лица человека и распознавание по признакам лиц.

Основные задачи систем видеонаблюдение со встроенной видеоаналитикой для обнаружения и контроля передвижения людей можно выделить следующие:

1. обнаружение человека на видео;
2. распознавание человека по лицу;

3. сопровождение передвижения человека на видео, полученного с одной камеры;

4. идентификация человека с определением всех его персональных данных;

5. повторная идентификация людей, изображения которых получены с разных камер или с одной, но в различное время.

Основные методы, которые могут использоваться для обнаружения движущихся людей

– межкадровой разности;

– вычитания фона

– на основе анализа оптического потока.

После того как человек обнаружен и выделен на изображении, необходимо выделить и распознать его лицо по средствам алгоритмов выделения лица человека на изображении (face detection).

Задачи видеоаналитики при распознавание лица человека по цифровому изображению происходит:

1) идентификации человека**.**

2) поиск местоположения человека в пространстве по его цифровой фотографии.

3) сопровождение по набору признаков, который включает, кроме признаков лица, общие признаки человека, позволяющие отследить его движение даже при невозможности распознавания лица. (например, когда оно скрыто капюшоном или расположено относительно видеокамеры под значительным углом, который не позволяет выполнить идентификацию по лицу.)

4) Далее следует поиск лиц в сопровождаемых областях. Выделение области поиска лица выполняется на основе анализа размеров детектированного фрагмента. Если его ширина меньше его высоты более чем в три раза, то анализируется только верхняя часть этого фрагмента, иначе анализируется вся область, описывающая человека.

Признаки лица используются для установления соответствия людей на кадрах, а также позволяет повысить эффективность при:

– сопровождения при анализе траекторий движения людей,

– долговременного скрытия их за объектами фона,

– высокой схожести внешних признаков людей.

Полученная на предыдущем шаге область кадра, содержащая лицо, поступает для распознавания. Для этого этапа применяется может применятся СНС MobileFaceNet, которая характеризуется значительно меньшими вычислительными затратами и обеспечивает при этом высокую точность работы (например, на базе данных LFW точность составляет 99,5%, а для СНС LResNet100E-IR – 99,77%).

Сопровождение людей (одного или нескольких человек)

На сегодняшний день наиболее результативным является сопровождение через обнаружение.

Алгоритмы классификации с применением СНС, устойчивы к изменениям:

– освещенности,

– динамическому заднему фону

– позволяют осуществлять детектирование даже в случае частичных перекрытий, что повышает качество сопровождения.

Если лицо не распознано *с использованием базы данных*, то должно выполнятся сравнение признаков обнаруженного лица с соответствующими данными **составного дескриптора.**

Составной дескриптор изображения каждого человека включает признаки лиц, вычисленные на основе СНС, и комплекс признаков изображения человека, что позволяет сопровождать людей даже при дальнейшей невозможности идентификации лиц.

В случаях невозможности обнаружения или распознавания лиц сопровождение выполняется на основе алгоритма, включающего: оценку наличия всей фигуры человека; формирование СНС-признаков для всей области и для верхней ее

части и их накопление; формирование пространственных признаков и фильтрацию по:

– расстоянию и размерам;

– вычисление схожести между всеми сопровождаемыми и обнаруженными на текущем кадре людьми и установление соответствия между ними;

– индексацию людей; определение их видимости на кадре;

– выделение рамкой человека при его присутствии в кадре.

Данная методика дает возможность идентифицировать

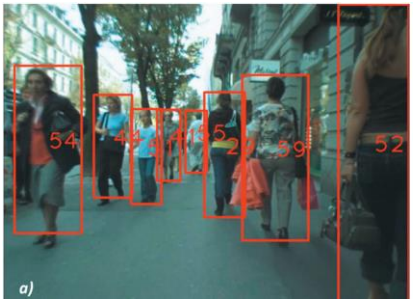
человека по лицу и затем сопровождать его передвижение при сложной траектории движения.

После того как лицо человека распознано, наступает этап полной идентификации человека с установлением всех его персональных данных. Это выполняется посредством поиска лица по базам данных, имеющим изображения лиц, например, «Образ +++».

Биометрические персональные данные

Риски

Распознавание человека *по лицу* можно использовать не только как инструмент для идентификации людей и отслеживания местоположения, но и для получения информации об их социальной активности (с кем и где они проводят время).



На примере опыта работы полиция города Чжэнчжоу, там сотрудники используют очки с системой распознания лиц, выдающие имя и адрес человека за 2-3 минуты. При этом если у человека есть профиль в социальных сетях (база его снимков разного возраста), то точность распознавания повышается.

Системы видеонаблюдения со встроенной видеоаналитикой необходимо использовать для распознавания лиц с полной идентификацией и даже с правовыми последствиями в виде штрафа, социального рейтинга и др.

Применение систем действительно приводит

1. к сокращению преступности,
2. предотвращению крупных аварий и т.д.,
3. посягательству на тайну частной жизни.

Вместе с тем, все большее распространение получает **добровольное согласие на «отслеживание»** путем использования различных приложений, определяющих и использующих геолокацию.

Закон «О защите персональных данных» (далее – Закон), должен внести определенную ясность в данную сферу. В Законе даются следующее определения:

– «**Биометрические данные»** – персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность;

– **«Персональные данные» –** сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

– Однако отсутствует понятие **«Идентификация физического лица»**

«Идентификация физического лица» – это когда физическое лицо может быть прямо или косвенно определено, (через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической,

психологической, умственной, экономической, культурной или социальной идентичности).

Преимущество определении заключается в том, что они четко описывает основные признаки персональных данных и позволяет относить к таким данным информацию, косвенно идентифицирующую субъектов персональных данных.

Законом, в частности, определяются биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение, голос и другое).

Таким образом, биометрических и физиологических данных большое количество, причем далеко не все активно используются с точки зрения сбора и последующей обработки. Во многих странах осуществляется сбор биометрических данных, таких как распознавание голоса и лица. Применение данных технологий возможно и в рамках электронного правительства при получении электронных услуг.

Необходимо принять закон **«Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных…»,** который будет регулировать отношения, возникающие при осуществлении идентификации с использованием биометрических персональных данных.

Изображение (фотография или видеосъемка) человека – это визуальные персональные данные, как подвид биометрических персональных данных, так как именно эти данные используются государством.

Сбор, обработка, хранение и даже передача этих данных, в том числе трансграничная, осуществляются повсеместно, начиная со сканирования и распознавания лица при использовании смартфона до полной идентификации человека на улице камерами видеонаблюдения.

Визуальные персональные данные становятся таковыми только после идентификации личности человека. Результаты видеосъемки в общественных местах или на охраняемой территории до установления личности **не считаются биометрией**. Только после распознавания и идентификации личности человека они становятся визуальными персональными данными.

Следует отметить, что использование систем видеонаблюдения возможно и без идентификации человека, в целом это касается общего мониторинга ситуации в городе. В случае выявления определенных отклонений от нормы (скопление людей, девиантное поведение, совершение противоправных действий) применяется технология распознавания лиц.

Контроль и защита визуальных персональных данных

Контроль и защита должна осуществляться со стороны оператора персональных данных

Изображение лица человека, распознанное системами видеоаналитики, может храниться в различных базах данных.

При утечке сведений из таких баз в Интернет они становятся доступными для всеобщего пользования. Люди должны быть уверены, что их визуальные персональные данные не будут

использованы в противоправных целях.

Персональные данные человека должны быть ***защищены.*** *Такая защита включает целую группу мер:*

– меры программного-технического характера (криптографическая защита, регламентация права на доступ и др.).

– меры организационно-правового характера: принятие нормативно-правовых актов, определяющих политику оператора в отношении обработки персональных данных, и ознакомление с ними сотрудников оператора,

– определение порядка доступа, внесение изменений в должностные обязанности лиц, обрабатывающих персональные данные, обучение сотрудников, назначение структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных,

– введение режима и охраны помещений, эффективного делопроизводства по электронным документам].

Обнародовать изображение гражданина – значит впервые сделать изображение доступным для всеобщего сведения. Однако обнародование изображения и его общедоступность не дают иным лицам права его свободно использовать *без получения согласия* изображенного лица.

Проблемой является использование баз данных с изображением лиц и людей для обучения нейронных сетей. При использовании существующих наборов данных, имеющихся в Интернете, для обучения СНС приходится сталкиваться с *проблемой защиты персональных данных*, и некоторые наборы данных являются закрытыми, так как авторы предоставляют для исследований не изображения, а только извлеченные из изображений людей признаки.

Если базу данных, содержащую фото людей, планируется кому-то передать и использовать, то необходимо, чтобы оператор выставил, а принимающая сторона подписала и соблюдала следующие условия:

– база данных не будет публиковаться, копироваться или распространяться каким-либо образом или в какой-либо форме, независимо от того, был изменен набор данных или нет;

– вся база данных будет использоваться только в целях научных исследований;

– изображения из базы данных не могут быть опубликованы или показаны в какой-либо форме для публикации, документа или демонстрации.

Для возможности использования изображений людей в исследовательских целях при формировании баз данных, содержащих фото, у всех участников необходимо получать разрешения на включение фото в базу. И такое разрешение должно быть в ***письменном виде***. Чтобы запросить и получить базу изображений для исследований, необходимо отправить подписанное соглашение держателям базы.

Контроль со стороны гражданина, с точки зрения гражданина важным является вопрос сбора, использования и дальнейшего распространения видео с его участием. Открытым остается вопрос присутствия человека в различных базах данных и **возможности от этого отказаться.**

Согласие субъекта персональных данных на обработку персональных данных, за исключением специальных персональных данных, не требуется: для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности; для исполнения правосудия, судебных постановлений и иных документов; в целях осуществления контроля (надзора) в соответствии с законодательными актами; для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно.

Основное требование законодателя к допустимости видеозаписи и фотосъемки заключается в том, что обе стороны должны быть осведомлены о ее проведении. Однако гражданин не знает, каким образом будет использована видеосъемка в последующем и будет ли произведена идентификация личностей. Использование и интегрирование такой информации, в базы данных будут признаваться *нарушением прав и свобод граждан*.

В рамках Закона о национальной безопасности Республики Казахстан, от 6 января 2012 года № 527-IV., информационная безопасность определена как – состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны;. *Таким образом, информационная безопасность личности является составной частью информационной безопасности*.

В связи этим необходимо соблюдать баланс интересов государства с точки зрения обеспечения общественной безопасности с использованием видеонаблюдения и последующей видеоаналитики и интересов человека, так как затрагиваются вопросы неприкосновенности частной жизни и персональных данных.

В соответствии с Законом любой человек вправе ***отозвать согласие***, а оператор обязан прекратить обработку и удалить информацию. Но данное право может быть реализовано только если этому ***предшествовало само согласие***.

Человек может требовать удаления своих данных, если их собрали или обработали без законных оснований. Остается открытым вопрос реализации данного права в части определения оператора. Если видео размещено в сети Интернет, то найти автора или первоисточник практически невозможно для простого пользователя. Если в результате опубликования фотографий или видеозаписи возникает *реальная угроза жизни и здоровью гражданина либо ему наносятся моральные страдания*, то на основании его мотивированного обращения распространение (демонстрация) данной информации должно быть прекращено.

Однако существует необходимость в разработке подзаконных актов, строго регламентирующих данную процедуру. На основании анализа зарубежного опыта выявляются следующие случаи использования изображения физического лица без его согласия:

– изображение человека относится к его публичной деятельности либо официальной должности;

– предоставление изображения человека по запросу правоохранительных органов;

– фиксация изображения человека в общественных местах.

Помимо указанных случаев использования изображения человека без его согласия, выявляется ограничительный принцип: использование изображения не должно унижать честь, достоинство и деловую репутацию человека, нарушать его

половую неприкосновенность, противоречить моральным устоям. Таким образом, необходимо разграничивать интересы государства в рамках обеспечения общественной безопасности и интересы личности в рамках защиты неприкосновенности частной жизни. Считаем, что на сегодняшний день существуют предпосылки для дальнейшего развития законодательства в сфере защиты персональных данных в части видеонаблюдения и выделения отдельного подвида биометрических персональных данных – визуальных персональных данных.

Архитектуры систем видеонаблюдения и видеоаналитики

В современных системных архитектурах для видеонаблюдения используются облачные технологии, концепция граничных вычислений (edge/fog computing) для обработки видеоданных в непосредственной близости от места их генерации и использования. Это позволит достичь высокой оперативности систем мониторинга безопасности за счёт снижения задержек при передаче видеопотоков по сети.

Камеры, разворачиваемые на границе сети, способны обрабатывать видеокадры в режиме реального времени, без передачи их в удалённое центральное облако. Граничные узлы способны интеллектуализировать сбор данных в зависимости от контекста событий перед видеокамерой.

Если на сцене ничего особенного не происходит, то частота кадров может быть снижена. Если в кадре начинается движение, видеокамера увеличивает частоту кадров, а если распознан инцидент – включает съёмку с высокой скоростью и в высоком разрешении. Это позволяет не только сэкономить полосу пропускания, но и вычислительные ресурсы, а также сократить требуемый объём систем хранения.

Устройства с видеоаналитикой можно настроить для решения следующих задач:

– поиск и классификация материалов по установленным параметрам;

– оповещение в режиме реального времени в случае обнаружения нарушений правил, что позволяет ускорить реагирование на возникшие угрозы;

– распознавание лиц и эмоций;

– подсчет количества людей в видеопотоке;

– подсчет времени нахождения в видеопотоке;

– анализ людей в видеопотоке, составление «белых» и «черных» списков;

– обработка черного списка интегрированная с POLY-FACE или образ +++ (т.е. лица находящихся в розыске или склонных к совершению. преступления).

Классификация программных средств анализа видеоизображения по типам

1. Детекторы движения

– Простейший детектор движения – регистрирует амплитуду и сигнала и площадь зоны детектирования

– Интеллектуальный детектор движения – функционально аналогичен простейшему детектору движения, но анализирует скорость, направление и характерные признаки цели

2. Биометрия движения

– Биометрия отдельных особенностей органов человека, размера руки, глаза, строение радужной оболочки или сетчатки глаза и т.д.

– Биометрия лица человека путем построения трехмерной модели

3. Система регистрации движущихся объектов
4. Борьба с терроризмом
5. Обнаружение возгорания
6. Наблюдение за технологическими процессами
7. Техническое зрение робототехники

Биометрия человека является наиболее надежным способом классификации человека. Она требует проведения определенных манипуляций от человека, что требует, как минимум, *согласия* на эти действия от проверяемого лица.

Биометрия путем построения двухмерной или трехмерной модели лица человека позволяет осуществлять контроль

дистанционно, однако здесь есть ограничения по применению, связанные с техническими возможностями данной технологии.

Методы распознавания лиц можно разбить на две группы:

– аналитические

– холистические.

Аналитические методы основаны на выделении геометрических признаков лица, описывающих его индивидуальные особенности.

В холистических методах рассматриваются общие свойства изображений человеческих лиц. Лицо распознается как нечто целое, а не состоящее из отдельных частей, таких как глаза, нос, рот, уши и т.п.

Искусственный интеллект

Операторы систем видеонаблюдения способны сохранять бдительность и внимательность в течение *короткого времени*, компьютер может обрабатывать большие объемы данных быстро.

Доступные на сегодняшний день системы ИИ не обучаются новым навыкам самостоятельно и не запоминают произошедшие события. Чтобы повысить эффективность системы, ее необходимо переобучить, используя более точные данные во время сеансов контролируемого обучения.

Неконтролируемое обучение обычно требует большого количества данных для создания кластеров и поэтому не используется в приложениях видеонаблюдения.

Большинство подходов, в видеонаблюдении связаны с «самообучением», основанных на анализе статистических данных, а не на фактическом переобучении моделей глубокого обучения.

Приложение на основе машинного обучения может успешно:

– бегущего человека (если оно было специально обучено этому), но в отличие от человека, который способен поместить данные в контекст,

– приложение не понимает, почему человек бежит: чтобы успеть на автобус или чтобы его не догнал полицейский?

Видеоаналитика не способна понимать, что происходит в кадре, с такой же проницательностью, как человек.

Видеоаналитика на базе искусственного интеллекта может выдавать *ложную тревогу или, в случае реального происшествия*, *не подавать сигналы*. Обычно такое происходит в сложной среде с интенсивным движением или когда человек несет крупный предмет, из-за которого приложение не может правильно классифицировать объект.

Видеоаналитика на базе ИИ на современном этапе должна использоваться как вспомогательный инструмент определения важности инцидента, прежде чем оповестить оператора, чтобы тот решил, как реагировать.

Таким образом, искусственный интеллект используется для обеспечения масштабируемости, а задача человека – оценивать потенциальные инциденты.

Факторы, определяющие эффективность видеоаналитики

Эффективность видеоаналитики зависит от множества факторов, большинство из которых можно оптимизировать.

К таким факторам относятся оснащение камеры, качество и динамические характеристики видеоизображения, уровень освещения, а также конфигурация, положение и направление камеры.

Пригодность изображения

Качество изображения зависит от высокого разрешения и высокой светочувствительности камеры, а также другие факторы, не менее важные при определении пригодности фото или видеозаписи.

Чтобы видеоаналитика работала надлежащим образом, камера должна быть расположена таким образом, чтобы зона наблюдения просматривалась полностью и беспрепятственно.

Пригодность изображения также может зависеть от сценария его использования. Качество видео, приемлемое для человеческого глаза, может быть недостаточно для приложения видеоаналитики.

Методы обработки изображений, обычно используемые для улучшения восприятия видео человеком, не рекомендуются при использовании видеоаналитики:

– методы шумоподавления.

– технология широкого динамического диапазона .

– и алгоритмы автоматического управления экспозицией.

– оснащение ИК-подсветкой.

Для получения точных результатов видеоаналитики необходимо «видеть» объект достаточно долго. Это время зависит от эффективности обработки (частоты кадров) платформы: чем она ниже, тем дольше объект должен находиться в кадре, чтобы его можно было обнаружить.

Если выдержка камеры не соответствует скорости движения объекта, точность обнаружения может пострадать из-за размытости изображения.

Быстрые объекты могут оказаться необнаруженными, если они перемещаются вблизи камеры.

Высокое разрешение камеры не означает большее расстояние обнаружения. Возможности обработки, необходимые для выполнения алгоритма машинного обучения, пропорциональны размеру входных данных. Очень часто из-за ограничений в возможностях обработки камерой в приложениях на основе ИИ используют более низкое разрешение, чем может предложить камера или видеопоток.

Настройка сигналов тревоги и записи

Из-за различных уровней применяемых фильтров аналитические приложения для обнаружения и классификации объектов генерируют очень мало ложных срабатываний.

В противном случае они могут пропустить важные события. Если все условия будут выполняться во всех без исключения случаях, рекомендуется использовать консервативный подход и настроить систему таким образом, чтобы конкретная классификация объектов не являлась единственной причиной срабатывания сигнала тревоги.

Такая настройка вызовет больше ложных срабатываний, но уменьшит риск пропустить важное событие.

Когда сигналы тревоги или инициирующие их срабатывание данные поступают непосредственно в ЦОУ или другие подразделения ОВД, каждая ложная тревога оборачивается большими расходами.

Совершенно очевидно, что необходима надежная классификация объектов, позволяющая отфильтровывать нежелательные сигналы тревоги. Однако механизм записи может и должен быть настроен так, чтобы полагаться не только на классификацию объектов.

В случае пропущенного *реального сигнала тревоги* эта настройка позволяет оценить по записи причину пропуска, а затем внести изменения в монтаж и конфигурацию всей системы. Если классификация объектов выполняется на сервере во время поиска инцидента, рекомендуется настроить систему на непрерывную запись и вообще не фильтровать исходную запись. Непрерывная запись занимает много места, но это в некоторой степени компенсируется современными алгоритмами сжатия, такими как Zipstream.

Алгоритмы глубокого обучения позволяют быстро решать сложные задачи с высокой, хотя и не 100%-ной точностью.

Во многих случаях результаты анализа дополняются уровнем достоверности, который в процентах показывает, насколько алгоритм уверен в том, что обнаруженный объект или событие соответствует описанию. Чаще всего такой подход применяется в системах распознавания лиц или номерных знаков.

С точки зрения правильности обнаружения возможны четыре ситуации:

– True positive – объект обнаружен, тревога активирована;

– True negative – объект не обнаружен, тревога не активирована;

– False positive – объект отсутствует, но обнаружен, активирована ложная тревога;

– False negative – объект присутствует, но не обнаружен, тревога не активирована.

Видеоанализ должен давать в основном результаты **True positive.** При слишком большом количестве ложных срабатываний сигналы тревоги в конце концов игнорируются. Важно также, насколько быстро событие или появление объекта обнаруживаются, особенно при анализе видео в реальном времени. Максимальная задержка обнаружения события или объекта в системе видеонаблюдения с оператором не должна превышать 1-2 с.

Независимо от того, какой объект наблюдается, общее эмпирическое правило состоит в следующем: чтобы можно было распознать детали объекта(ов), размер картинки должен быть не менее 30-50 пикселей.

Криминалистические исследования проводимые для идентификации человека

К установлению личности по признакам внешнего облика чаще всего прибегают органы досудебного расследования при проведении:

1. оперативно-разыскных мероприятий (наблюдение, отождествление личности, проверка по учету субъективных портретов);

2. следственных действий (допрос, предъявление лица для опознания и назначение портретной экспертизы);

3. производстве судебно-портретных исследований (экспертиз).

Биометрическая идентификация личности, являясь одним из методов распознавания или аутентификации человека, имеет некоторые отличия от криминалистической идентификации личности. Они создаются с целью ограничения доступа к информации, предотвращения проникновения злоумышленников на охраняемые территории и в помещения, для защиты от подделки электронных идентификационных документов и т.д.

Существует три традиционных способа аутентификации:

1. по собственности – физическим предметам, таким, как ключи, паспорт и смарт-карты;

2. по знаниям информации, которая должна храниться в секрете и которую может знать только определенный человек, например пароль;

3. по биометрическим параметрам – физиологическим или поведенческим характеристикам индивида. Это части человеческого тела или действия, по которым можно отличить людей друг от друга.

Биометрические технологии можно разделить на две ветви.

1. группа технологий, построенных на анализе статических (неизменяемых) образов личности, данных ей от рождения и хорошо наблюдаемых окружающими (особенности геометрии лица, руки, отпечатка пальца, структура глаза).

2. биометрические программы, построенные на анализе динамических образов личности, которые отражают особенности характерных для неё быстрых подсознательных движений (динамические параметры письма, голос человека, его походка).

К биометрическим технологиям, основанным на анализе статистических образов личности (физиологических), относятся:

1. Идентификация на основе папиллярных рисунков пальцев рук. На долю использования этого параметра приходит большинство существующих биометрических систем.

2. Идентификация по индивидуальным особенностям геометрии лица основывается на применении методов габитоскопии.

3. Идентификация по рисунку радужной оболочки глаза производится путем измерения и анализа цветного кольца вокруг зрачка глаза.

4. Идентификация по силуэту кисти руки. Данные биометрические технологии основаны на измерении длины и ширины пальцев руки, появились одними из первых более 25 лет назад.

5. Идентификация по рисунку кровеносных сосудов глазного дна. Является одним из наиболее новых и достаточно надёжных методов идентификации.

6. Идентификация по термограмме лица (схеме артерий, снабжающих кожу лица тёплой кровью) - осуществляется с использованием специализированной видеокамеры дальнего инфракрасного диапазона.

7. Идентификация по венам руки производится по рисунку вен тыльной стороны кисти руки, сжатой в кулак.

К биометрическим технологиям, основанных на анализе динамических образов личности (поведенческих), составляют:

1. Идентификация по голосу - метод, который основывается на распознавании таких уникальных свойств голоса, как частота, модуляция, интонация и т.д.

2. Идентификация по рукописному почерку осуществляется на основе анализа характерных для личности быстрых подсознательных движений.

3. Идентификация человека по динамическим проявлениям внешнего облика, как походка, мимика, артикуляция, жестикуляция.

Биометрические технологии основаны на автоматизированных системах, осуществляющих следующие функции:

1. получение и хранение в базе данных оцифрованного образца биометрической характеристики индивида;
2. введение в систему проверяемой характеристики человека;
3. извлечение индивидуализирующих признаков;
4. сравнение признаков введенной характеристики с признаками образца из базы данных;
5. заключение о тождестве или различии сравниваемых биометрических характеристик.

К основным сферам внедрения биометрических технологий идентификации личности следует отнести:

– осуществление пограничного и паспортного контроля,

– использование в работе иммиграционных служб,

– при проведении оперативно-разыскной деятельности,

– в системе криминалистической регистрации

– при проведении криминалистических исследований (экспертиз) и т.п.

Оперативно-розыскная деятельность, Биометрические технологии, позволяющие осуществлять дистанционно и незаметно для объекта идентификацию его личности, которые интегрированы в системы видеонаблюдения.

Криминалистическая регистрация. Различные биометрические данные, индивидуализирующие человека, которые ранее не использовались в системе криминалистической регистрации, могут также фиксироваться в базах данных для получения информации.

Материалы содержащие биометрическую информацию

Например: потожировые следы пальцев, голос, профиль ДНК, (выделенный из слюны, оставленной на ободке чашки)

Криминалистическая биометрическая информация» позволяет:

– подтвердить или опровергнуть причастность лица к правонарушению путем предоставления – как

самостоятельно, так и в составе других доказательств – данных, либо подтверждающих вину, либо освобождающих от обвинения

– обеспечить проведение объективного и убедительного судебного процесса на принципах верховенства закона, снизив зависимость от признаний, полученных в ходе расследования

– дать картину событий, происходивших на месте преступления и в связи с ним;

– найти связь данного лица с деянием, событием, местом или другим лицом до инцидента, в его ходе или после него;

– найти связь одного события с другим;

– выявить данные, находящиеся в различных электронных или цифровых системах, и найти связь между ними.

Криминалистическое исследование динамических признаков человека», является изучение теоретических основ по идентификации динамических проявлений человека, зафиксированных средствами и приборами видео наблюдения с последующим установлением личности.

Криминалистические исследования динамических признаков человека отнесены к портретным исследованиям.

Под термином портрет понимается изображение или описание какого-либо человека либо группы людей, существующих или существовавших в реальной действительности, где (изображенные или описываемые) объекты и их признаки находятся в неподвижном состоянии.

В то время как динамические признаки человека проявляются в движении.

При исследовании динамических признаков человека или группы людей, в отличие от портретного, элементам и признакам изучаемого объекта присуще свойство динамичности.

Криминалистически значимая информация о динамических признаках человека по форме проявления динамических элементов походки и их признакам делятся на две группы:

1. относятся проявления, «которые могут отображаться в виде материально фиксированных следов (в статике);

2. относятся отличительные признаки, воспринимаемые только в динамике и соответственно зафиксировать их можно только с помощью средств видеозаписи».

Под динамическими признаками человека принято понимать:

1. проявления внешних особенностей человека в виде двигательной активности

2. анатомические элементы облика воспринимаемые визуально или фиксируемые с помощью средств видеозаписи.

Общая классификация построения системы динамических признаков человека с позиции экспертно-криминалистической идентификации включает в себя:

1. динамические двигательные признаки, связанные с перемещением тела в пространстве и его ориентацией;

2. динамические коммуникативные признаки (динамика изменения мимики лица, артикуляции речевого аппарата, жестикуляции и т.д.);

3. динамические признаки человека, проявляются в реализации его навыков (трудовых, спортивных, преступных) и привычек.

К видами динамических признаков, используемых в габитоскопических исследованиях, являются – походка, мимика, жестикуляция, артикуляция, двигательные проявления навыков и привычек человека.

Важным динамическим элементом человека является его способность передвигаться путем ходьбы и беге, различия в которых заключается *в скорости передвижения.*

Походка для каждого человека является сугубо индивидуальной и формируется в течение всей жизни при помощи создания нервно-мышечного автоматизма под постоянным контролем нервной системы путем образования устойчивых условно-рефлекторных связей.

*Уникальность **«динамических образов»** движений является:*

1. антропоморфологическое различие людей

2. привычки заложенные в раннем детстве в ходе обучения и формирования динамического вариотипа этого навыка.

Особенности (отличительные признаки) походки зависят от – возраста, пола, патологий опорно-двигательного аппарата (в силу различных заболеваний, травм), состояния, одежды, обуви, наличия спортивных, профессиональных или иных навыков, переносимого груза, условий и целей ходьбы и других факторов.

К первой группе динамических элементов и их признаков относятся: длина шага, ширина шага, положение и постановка стоп при ходьбе, которые могут быть исследованы.

Ко второй группе относятся следующие динамические элементы и их признаки: темп (скорость), равномерность, симметричность ходьбы, степень поднимания стоп при ходьбе, степень сгибания коленей, особенности положения и движения головы, туловища, рук и т.д.

Динамические элементы походки и их отличительные признаки, относящиеся ко второй группе, ранее не исследовались по причине отсутствия технических средств, методик для проведения измерений и таким образом получения количественной информации о них.

Наличием у человека биологических и функциональных асимметрий, оказывают влияние на походку в виде различий в амплитудах движений симметричных частей тела.

При описании внешности человека выделяются от 6 до 29 различных видов походки и движений тела.

При описании ходьбы рассматриваются ее скорость, равномерность, симметричность, отмечаются размер шага, расстановка ног в стороны, положение и постановка стоп при ходьбе, степень их отрывания от земли, степень сгибания коленей.

Для характеристики походки используется совокупность этих признаков, а также положение и движение головы, плеч, туловища, таза, рук». Классификация походки:

– по темпу движения: быстрая, «поспешная», торопливая, деловая, расслабленная, неторопливая, суетливая;

– по степени поднимания стоп и сгибания коленей: «подпрыгивающую», «пружинистую», «танцующую», «на цыпочках», «журавлиную», семенящую;

– по положению и постановке стоп: спотыкающуюся, «лисью» и «косолапую»;

– по положению и особенностям движении туловища, головы, плеч, рук.

Отождествление личности по следам ходьбы должно базироваться на:

– установлении и сопоставлении устойчивых индивидуально выраженных закономерных соотношений между отдельными элементами дорожек следов ходьбы;

– на установлении того, что эти закономерности характеризуют анатомо-физиологические особенности отождествляемого лица.

Теоретические подходы идентификации динамических элементов и их признаков по походке, реализуются на основе целого комплекса полученной из разных источников информации, характеризующих те или иные свойства и проявления личности (биологические, социально-демографические, функциональные, медицинские, психолого-психиатрические и др.).

Необходимо обобщить динамические признаки походки человека в единый комплекс информации с дифференциацией по следующим категориям:

– медицинские особенности;

– профессиональные особенности и навыки;

– физиологические особенности (врожденные).

Средством фиксации динамических признаков человека являются современные системы видеонаблюдения в виду присущих им следующих свойств:

– объективности информации (передаваемых в виде материально-фиксированных отображений внешности человека);

– высокого разрешения качества изображения;

– резкостью кадра, делающих их пригодными для дальнейшего экспертного исследования;

– совместимостью (с различными компьютерными программами и технологиями.

Анализ информации запечатленной на видеоносителе о динамических проявлениях человека имеет последовательность, включающую следующие этапы:

– перенос видеоизображения в память компьютера;

– разбивка видеоизображения на отдельные кадры;

– нанесение на каждое из статических изображений видеоряда пространственных координат;

– разметка на каждом из статических изображений антропометрических точек, соответствующих частям тела или элементам внешности человека;

– измерение значений отличительных динамических признаков человека;

– статистическая и математическая обработка результатов измерения динамических признаков человека.

Особенности криминалистической идентификация человека по видеоизображениям:

1. Криминалистическая идентификация человека по признакам анатомических элементов внешнего облика, запечатленным на видеоизображениях, – это процесс установления наличия или отсутствия тождества человека по признакам анатомических элементов внешнего облика по материально-фиксированным отображениям (видеоизображениям), осуществляемый путем производства судебно-портретной экспертизы.

2. Классификация факторов, влияющих на отображение признаков анатомических элементов внешнего облика человека, запечатленных на видеоизображениях:

– факторы материальной части средств видеозаписи

– факторы процесса записи видеоизображения на носителях

– факторы условий видеозаписи

– факторы состояния внешности объекта запечатления

– факторы условий хранения видеозаписи.

3. Формирование видеоучетов отображений признаков анатомических элементов для использования при проведении оперативно-разыскных мероприятий и выполнения индивидуально-профилактических функций в отношении подучетных лиц.

4. Классификация видеоизображений анатомических элементов внешнего облика, получаемых в качестве образцов для сравнительного исследования:

– по виду видеозаписывающего устройства, с помощью которого может быть получено видеоизображение;

– по формату видеозаписи;

– по формату сжатия видеозаписи;

– по субъекту получения;

– по процессуальному положению лица, изображение которого используется

– в качестве отображения внешнего облика человека;

– по связи с уголовным делом;

– по содержанию;

– по значимости для идентификации человека по признакам элементов внешнего облика.

5. Методика судебно-портретной экспертизы с использованием видеоизображений, должна включать в себя:

– специфику определения пригодности видеоизображения для идентификации человека по признакам внешности;

– при проведении раздельного исследования необходимо решать вопрос о суммировании видеокадров, на которых получили отображение признаки анатомических элементов внешности человека с целью получения пригодного для идентификации комплекса этих признаков;

– при оценке результатов сравнительного исследования предложены критерии формулирования того или иного вывода при производстве портретной экспертизы по видеоизображениям.

6. Классификация совокупностей признаков элементов внешнего облика человека при оценке результатов сравнительного исследования:

1. по объективному отображению (достоверные, мнимые);
2. по полноте отображения (полные, частичные);
3. по степени значимости (существенные, несущественные);
4. по характеру устойчивости (устойчивые, неустойчивые);
5. по степени встречаемости в группе людей (групповые, индивидуальные);
6. по объективной сущности (качественные, количественные);
7. по объему (достаточные, недостаточные).

Отождествление человека по видеоизображениям и фотоснимкам является одним из наиболее сложных видов криминалистической идентификации. Это обусловлено, прежде всего, относительной ограниченной информативностью сравниваемых объектов.

Полнота и достоверность отображения признаков внешности при видеосъемке зависит от следующих факторов:

– технических характеристик видеокамеры;

– условий съемки;

– масштаба изображения головы человека, расположение ее по площади кадра;

– положения запечатлеваемого объекта относительно видеокамеры;

– способ выполнения видеосъемки.

На полноту отображения признаков внешности влияют технические характеристики видеоаппаратуры, монитора, и способы получения твердой копии с кадра.

На качество изображения на видеоносителе влияют:

– помехи видеосигналов в виде сетки, муара, полос;

– искажение временного масштаба видеосигнала (искажаются размерные характеристики изображения);

– цветопередача (понижение насыщенности и потеря цвета приводят к искажению цвета элементов внешности)

Задачами при производстве портретной экспертизы является

– изучение и сопоставление видеоизображений, полученных с видео – контрольных устройств. Это связано с тем, что элементы и признаки внешнего облика человека, отобразившиеся на такого рода объектах имеют геометрические искажения пропорций, часть мелких признаков не отображается.

Существенной причиной затрудняющий производство экспертиз по видеоизображением является невысокое качество представленных на исследования видеокадров и отсутствие при сравнении фотоснимков и видеоизображений (при наличии подозреваемого) сопоставимого материала.

– влияния условий видеосъемки на полноту и достоверность отобразившихся признаков;

– наиболее эффективные методы, используемые на стадии сравнительного исследования.

– освещение лица в момент видеосъемки оказывает существенное влияние на отображение его особенностей.

– влияние дистанции видеосъемки на достоверность и полноту отображения признаков внешности на видеоизображениях.

– качество, которое зависит от разрешающей способности видеокамеры.

Алгоритм действий по подготовке сравнительного материала при выполнении экспертиз по видеоизображениям:

1. внимательно просмотреть представленную на исследование видеозапись.

2. выбрать на представленной видеозаписи видеокадры, на которых наиболее полно и достоверно отобразились анатомические элементы и признаки.

3. привести видеоизображения к одному масштабу и распечатать их на твердом носителе (фотобумаге).

4. разработать сценарий действий подозреваемого с учетом отобранных видеокадров.

5. произвести фотосъемку подозреваемого по разработанному сценарию с максимальным разрешением.

6. привести представленные изображения к одному масштабу.

Правовые и этические нормы в сфере видеоаналитики с применением искусственного интеллекта

Правовое регулирование видеоаналитики с использованием искусственного интеллекта (ИИ) основывается на законодательных актах и нормативных документах, направленных на защиту персональных данных, обеспечение безопасности и регулирование использования ИИ.

1. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года №94-V.

– Регулирует порядок сбора, обработки и хранения персональных данных, включая данные, получаемые с использованием видеоаналитики.

– Требует от организаций получения согласия субъектов данных на обработку их персональных данных.

– Определяет меры по защите персональных данных от несанкционированного доступа, утраты, изменения и других угроз.

2. Закон Республики Казахстан «О доступе к информации» 16 ноября 2015 года №401-V:

– Устанавливает требования к информационной безопасности при использовании систем видеоаналитики.

– Включает положения о защите информации в системах видеонаблюдения и видеоаналитики, а также о предотвращении утечек данных.

3. Закон Республики Казахстан «О связи» Закон Республики Казахстан от 5 июля 2004 года №567.:

– Регулирует вопросы, связанные с передачей данных, включая видеоинформацию, через сети связи.

– Определяет ответственность операторов связи за защиту передаваемых данных.

4. *Инструкция по организации надзора за законностью деятельности государственных, местных представительных и исполнительных органов, органов местного самоуправления и их должностных лиц, иных организаций независимо от формы собственности, а также принимаемых ими актов и решений, судебных актов, вступивших в законную силу, исполнительного производства, представительства интересов государства в суде по гражданским и административным делам от 2 мая 2018 года №60*

– Включает положения о надзоре за соблюдением законодательства в сфере обработки и защиты персональных данных.

– Определяет полномочия государственных органов в области контроля за использованием систем видеоаналитики.

5. Приказ Председателя Комитета национальной безопасности Республики Казахстан от 27 октября 2020 года №69. Правила функционирования Национальной системы видеомониторинга

6. Дополнительные документы и стандарты:

– Стандарты и нормы в области защиты информации включающие технические и организационные меры по защите данных, используемых в системах видеоаналитики.

– Инструкции и методические рекомендации государственных органов определяющие конкретные процедуры и требования к использованию систем видеоаналитики, включая использование ИИ.

Особенности правового регулирования:

1. Получение согласия субъектов данных:

– Обязательное получение согласия на сбор и обработку данных при использовании систем видеоаналитики.

– Информирование лица о целях и способах обработки их данных.

2. Защита данных:

– Обеспечение конфиденциальности, целостности и доступности данных.

– Применение мер по защите данных от несанкционированного доступа и утечек.

3. Прозрачность и ответственность:

– Предоставление субъектам данных информации о том, как их данные обрабатываются.

– Установление ответственности за нарушение законодательства в области защиты персональных данных.

4. Государственный контроль и надзор:

Осуществление контроля за соблюдением законодательства в области видеоаналитики и защиты персональных данных.

Проведение проверок и аудитов систем видеоаналитики на соответствие требованиям законодательства.

В целом, правовое регулирование видеоаналитики с использованием ИИ в Казахстане направлено на обеспечение защиты персональных данных, информационной безопасности и соблюдения прав граждан при использовании современных технологий.

Крайне важным является правовое регулирования систем общественной безопасности таким образом, чтобы обеспечить соблюдение права на неприкосновенность частной жизни, не допустить произвольного вмешательствав жизнь человека.

Этический вопрос «вторжения» систем видеонаблюдения и видеоаналитики в частную жизнь каждого отдельного добропорядочного гражданина, на которое он не давал своего предварительного согласия, заслуживает отдельного обсуждения.

Главный правовой вопрос можно сформулировать довольно быстро: насколько это в принципе согласуется с нормами основного закона страны – Конституции.

К настоящему времени в стране функционирует достаточно большое количество баз данных, содержащих как персональные, так и иные данные в отношении каждого человека. Так, создана и функционирует государственная централизованная автоматизированная информационная система «Правительство для граждан», основу которой составляет база персональных данных граждан, иностранных граждан и лиц без гражданства, постоянно проживающих в Республике Казахстан.

В связи с этим применение систем ИИ позволяет не только распознать лицо человека, но и получить всю

информацию о нем путем выборки, которая содержится во всех базах данных страны.

Необходимо определить четкий правовой механизм сбора и защиты персональных данных и частной жизни в части получения данной информации:

1. обозначить цели, для которых возможно использование информации с камер видеонаблюдения;
2. определить круг лиц, имеющих доступ к базам с обязанностью сохранности данной информации в тайне и ответственности за ее разглашение;
3. строго регламентировать порядок доступа иных лиц;
4. обеспечить эффективную техническую защиту (в том числе идентификация пользователей системы);
5. получать согласие лица на сбор и обработку данных и др.

Кроме того, в современных условиях недостаточно проработанным и понятным для простого гражданина является *механизм защиты его прав в случае их нарушения.*

Необходимо информировать граждан, почему и с какой целью государственные органы применяют системы видеоаналитики с применением ИИ. Прозрачность и обмен информацией играют важнейшую роль для эффективной работы систем видеоаналитики.

Заключение

В настоящее время применение систем видеонаблюдения является неотъемлемым признаком развитых стран, движущихся по пути построения «умных» городов. В эпоху развития искусственного интеллекта возможности данных систем не ограничиваются просто съемкой или обезличенным видеонаблюдением, а предоставляют возможности распознавания и полной идентификации человека. В связи с тем, что процесс информатизации привел к созданию многочисленных баз данных, включая автоматизированные информационные системы персональных данных, интеграция баз данных с системами видеонаблюдения в том числе видеоаналитики является вопросом времени.

Полная идентификация человека станет возможной в автоматическом режиме, положительный аспект применения систем видеоаналитики: сократил количество противоправных действий, повысилась раскрываемость преступлений

Вопросы неприкосновенности частной жизни и обеспечения информационной безопасности личности выходят на первый план. Потому необходимо на правовом уровне обеспечивать баланс интересов государства и личности.

Использования систем видеонаблюдения государством, следует обеспечить защиту на техническом, организационном (строгая регламентация доступа, ответственность лиц, имеющих доступ к системам, и др.) и правовом (с точки зрения защиты права на неприкосновенность частной жизни) уровнях.

С учетом имеющихся технических возможностей и с использованием общедоступных персональных данных, распространенных самим человеком, идентификация человека также возможна. Дальнейшее совершенствование законодательства в сфере защиты персональных данных путем выделения отдельного подвида – визуальных персональных данных – и разработки правового регулирования в данной сфере.

Список использованной литературы

1. Орлов П.Г. Идентификация личности по фотокарточкам: Пособие. – М.: ВКШ КГБ СССР. 1974. – С. 59; Зинин А.М., Подволодский И.Н. Габитоскопия: Учебное пособие. – М.: Юрлитинформ, 2006. – С. 34 и др.Селиванов Н.А., Танасевич В.Г., Эйсман А.А. и др. Советская криминалистика. Теоретические проблемы, – М.: Изд-во «Юридическая литература», 1978. – С. 125.
2. Закон О персональных данных и их защите ЗРК от 21 мая 2013 года N94-V. (с изменениями и дополнениями по состоянию на *20.06.2024*г.) https://adilet.zan.kz/rus/docs/Z1300000094
3. Приказ Председателя Комитета национальной безопасности Республики Казахстан от 27 октября 2020 года №69. – Об утверждении Правил функционирования Национальной системы видеомониторинга [Электронный ресурс] https://adilet.zan.kz/rus/docs/V2000021693
4. Моисеева Т.Ф. Биометрические технологии в аспекте экспертных исследований // Сборник статей: Актуальные проблемы теории и практики уголовного судопроизводства и криминалистики. Часть III: Вопросы теории и практики судебной экспертизы. – М.: Академия управления МВД России, 2004. – С. 56-59
5. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений: Монография. – Пенза: Изд-во Пенз. гос ун-та, 2000. – С. 16- 17.
6. Барсуков В.С., Зайцев А.В., Пономарев А.А. Идентификация личности – ключевая проблема безопасности // Специальная техника. – 2005. – № 3. – С. 32-40.
7. Сафонов А.А., Булгаков В.Г., Варченко И.А. Криминалистическое исследование динамических признаков человека: история и современное состояние//Общество и право. 2010 №3(30) – С. 250-257.

8. Судебная портретная экспертиза на современном этапе. Проблемы и пути решения: Материалы Всероссийской конференции (28 февраля 2017 года). – М.: Научно-практический журнал «Энциклопедия Судебной Экспертизы». № 2 (13) 2017 – С. 221.; Судебная портретная экспертиза на современном этапе. Проблемы и пути решения: Материалы Всероссийской конференции (29 ноября 2018 года). – М.: Энциклопедия Судебной Экспертизы: Научно-практический журнал. №4 (19) 2018. – С. 214.

9. Использование криминалистически значимой информации о динамических признаках человека в раскрытии и расследовании преступлений: монография / под ред. докт. юрид. наук, проф. А.М. Зинина. – М.: Юрлитинформ, 2013. – С. 160.

10. Дильбарханова Ж. Р. Криминалистическое исследование внешнего облика человека: учебно-практическое пособие. – Алматы: Юрист, 2008. – С. 100.

11. Булгаков В. Г., Булгакова Е. В. Роль информации о динамических признаках человека в розыскном портрете неизвестного преступника//Вестник Волгоградского государственного университета. Серия 5, Юриспруденция, 2011 №2 (15), – С. 149-152.

12. Rissland E.L. Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning // Yale Law Journal. 1990. Vol.99. No.8. P.1957-1981. [Электронный ресурс] (дата обращения:06.06.2024)

13. Ashley K.D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge University Press. 2017. 450 p. [Электронный ресурс] (дата обращения:09.07.2024)

14. Stone P. et al. Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016. Stanford. Stanford University. 2016. 52 p.

15. Шрейнер И.Ю. Внедрение системы «умный город» для повышения безопасности городской среды / И.Ю. Шрейнер, И.С. Пашкова // Безопасность городской

среды : материалы IV Междунар. научно-практ. конф., Омск, 16-18 нояб. 2016г. – Омск : Омский гос. техн. ун-т, 2017. – С. 314–316. [Электронный ресурс] (дата обращения:06.06.2024)

16. Климович А.П. Влияние цифровых технологий на современное общество. Пример системы рейтинга социального кредита в Китае / А.П. Климович // Цифровая социология. – 2020. – Т. 3. – № 3. – С. 35–44.

17. Богуш Р.П. Алгоритм сопровождения людей на видеопоследовательностях с использованием сверточных нейронных сетей для видеонаблюдения внутри помещений / Р.П. Богуш, И.Ю. Захарова // Компьютерная оптика. – 2020. – Т.44. – №1 – С. 109–116. doi: 10.18287/2412-6179-CO-565.

18. Богуш Р.П. Обнаружение объектов на изображениях с большим разрешением на основе их пирамидально-блочной обработки / Р.П. Богуш, И.Ю. Захарова, С.В. Абламейко // Информатика. – 2020. – №2 – С. 7-16. doi:10.37661/1816- 0301-2020-17-2-7-16.

19. «Facing the Camera -The Protection of Freedoms Act 2012 & The Surveillance Camera Code of Practice».- Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales 2020 [Электронный ресурс] (дата обращения : 04.07.2024).

20. Li W., Zhao R., Xiao T., Wang X. Deep Filter Pairing Neural Network for Person Re-identification. DeepReID: IEEE Conference on Computer Vision and Pattern Recognition. 2014. P. 152-159. Available from: https://doi.org/10.1109/ CVPR.2014.27. [Электронный ресурс] (а дата обращения: 10.08.2024).

21. Абламейко М.С. Защита визуальных персональных данных: правовые аспекты / М.С. Абламейко // Вебпрограммирование и интернет-технологии WebConf2021:

материалы 5-й Международной научно-практической конференции, – Минск, 18-21 мая 2021г. / БГУ, Механико-математический фак.; редкол.: И.М. Галкин (отв. ред.) [и др.]. – Минск: БГУ, 2021. – С. 400. – Деп. в БГУ 07.05.2021, №005207052021. [Электронный ресурс] (дата обращения: 05.09.2024).

22. Сайдамарова В.В., Бубербаев Н.Д.: Криминалистический анализ использования камер видеонаблюдения в досудебном расследовании при идентификации человека – Караганда: КА МВД РК им. Б. Бейсенова, 2020. – С. 10.

СОДЕРЖАНИЕ

Верстка:
Туренова Б.Ю.

Отдел организации научно-исследовательской и редакционно-издательской работы Алматинской академии МВД Республики Казахстан
имени М. Есбулатова 050060 Алматы, ул. Утепова, 29

Подписано в печать 13 декабря 2024 г.
Формат 60x84 1/16 Бум. тип. №1. Печать на ризографе. Уч.-изд. п.л. 1,9.
Тираж 50 экз.