Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2023. № 3
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)
Компьютерное обеспечение и вычислительная техника

Научная статья
УДК 004.8
https://doi.org/10.24143/2072-9502-2023-3-76-86
EDN RNNIFE

Система событийного мониторинга для автоматизированного обнаружения инцидентов

И. М. Космачева✉, И. Ю. Кучин, Н. В. Давидюк, М. Ф. Руденко, В. И. Лобейко, И. В. Сибикина

Астраханский государственный технический университет,
Астрахань, Россия, ikosmacheva@mail.ru✉

Аннотация. В настоящее время пользуются повышенным интересом технологии компьютерного зрения, применяемые в системах событийного мониторинга для решения задач обеспечения безопасности в сфере транспорта, медицины, защиты данных. Системы видеонаблюдения ежедневно формируют петабайты данных, а в процессе обработки используется лишь малая их часть. Использование видеоаналитики избавит от необходимости хранения и обработки лишних данных, их ручного просмотра, что напрямую повлияет на стоимость, трудоемкость и скорость решения оперативных производственных задач реагирования на инциденты. Данные с видеокамер и другая информация, собранная из разных источников, совместно использованные для анализа, позволили бы более эффективно и оперативно выявлять и предупреждать различные нежелательные события. Автоматизировать анализ сложноструктурированных данных, снижая влияние человеческого фактора, исключая ошибки и злоупотребления, можно с помощью методов искусственного интеллекта, нейронных сетей. Но современные интеллектуальные системы видеоаналитики не лишены недостатков. Многие системы ориентированы на распознавание какого-то определенного типа изображений, могут работать в ограниченных предметных областях и с определенными условиями внешней среды. Алгоритмы распознавания связаны с большим количеством ложных срабатываний, особенно в условиях стремительного увеличения объема данных, степени неопределенности входной информации, поэтому предлагается дополнять системы событийного мониторинга. Системы содержат большое количество настроек, правил, что тоже усложняет понимание работы системы. Описываются сложности использования биометрических данных в системах распознавания в связи с правовыми ограничениями, основные этапы проектирования системы событийного мониторинга, представлена ее модель, объединяющая в себе элементы нечеткой логики и методов распознавания образов.

Ключевые слова: правило, детектор, видеоаналитика, данные, параметры, безопасность

Для цитирования: *Космачева И. М., Кучин И. Ю., Давидюк Н. В., Руденко М. Ф., Лобейко В. И., Сибикина И. В.* Система событийного мониторинга для автоматизированного обнаружения инцидентов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2023. № 3. С. 76–86. https://doi.org/10.24143/2072-9502-2023-3-76-86. EDN RNNIFE.

Original article

Event monitoring system for automated incident detection

I. M. Kosmacheva✉, I. Yu. Kuchin, N. V. Davidyk, M. F. Rudenko, V. I. Lobeyko, I. V. Sibikina

Astrakhan State Technical University,
Astrakhan, Russia, ikosmacheva@mail.ru✉

Abstract. Currently, computer vision technologies used in event monitoring systems to solve security problems in the field of transport, data protection, medicine are becoming an increasingly promising direction. Video surveillance systems generate petabytes of data every day, and only a small part is used in processing. The use of video analytics will eliminate the need for storing and processing unnecessary data, their manual viewing, which will directly affect the cost, complexity and speed of solving operational production tasks of responding to incidents. The data from video cameras, information collected from different sources and used together for analysis would make it possible to more effectively and quickly identify and prevent various undesirable events. It is possible to automate the analysis of complex structured data, reducing the influence of the human factor, eliminating errors and abuses, using artificial intelli-

gence methods, neural networks. But modern intelligent video analytics systems have drawbacks. Many systems are focused on the recognition of a certain type of images, can work in limited subject areas and under certain environmental conditions. Recognition algorithms are associated with a large number of false positives, especially in conditions of a rapidly increasing data volume, the degree of uncertainty of input information, therefore, it is proposed to supplement event monitoring systems. The systems contain a large number of settings and rules, which complicates the understanding of the system. There have been described the difficulties of using biometric data in recognition systems due to the legal restrictions, the main stages of designing an event monitoring system, its model, which combines elements of fuzzy logic and pattern recognition methods.

Keywords: rule, detector, video analytics, data, parameters, security

For citation: Kosmacheva I. M., Kuchin I. Yu., Davidyk N. V., Rudenko M. F., Lobeyko V. I., Sibikina I. V. Event monitoring system for automated incident detection. *Vestnik of Astrakhan State Technical University. Series: management, computer science and informatics*. 2023;3:76-86. (In Russ.). https://doi.org/10.24143/2072-9502-2023-3-76-86. EDN RNNIFE.

Введение

Видеоаналитика (ВА) – это технология, использующая методы компьютерного зрения для автоматизированного получения данных на основании анализа изображений или последовательностей изображений (видеопотоков).

Современные системы компьютерного зрения интегрируются в различные системы управления и принятия решения. С их помощью можно контролировать каналы утечки данных, связанные с несанкционированной съемкой секретных данных с рабочего экрана компьютера или с бумажных носителей в организации. Такой канал утечки данных всегда было трудно контролировать. Оперативное наблюдение за объектами, процессами, явлениями, свойствами объектов необходимо и для решения таких хозяйственных задач, как контроль над ходом половодья на реках, мониторинг нефтяных загрязнений на водной поверхности или почве [1, 2], распознавание активности учеников на экзамене (чтение, использование запрещенных предметов, желание что-то спросить).

Происходит совершенствование алгоритмов распознавания событий/объектов и расширение применения разнообразных типов сенсоров (микрофоны, тепловизоры, GPS/ГЛОНАСС) для регистрации признаков обнаруживаемого инцидента.

Под объектом наблюдения понимается контролируемый периметр, человек, транспортное средство, животное, предмет, процесс или явление (пожар, разлив реки и т. д.) в зоне наблюдения. Можно использовать алгоритмы, чтобы объединять отдельные объекты в более крупные производные – толпа, транспортная «пробка», движение. Современные IP-камеры способны обнаружить движение и его направление, лица или толпу, номера автотранспортных средств, факты саботажа – закрытия телекамеры или ее сдвиг. Важной функцией видеоаналитики является возможность сбора статистики для подсчета людей в видеопотоке, составления тепловых карт и определения пола и возраста объектов наблюдения [3].

Обработка большого объема разнородных данных в сложных системах в условиях неопределенности эффективна на базе нечеткой логики с применением системы правил.

Системы правил для срабатывания в ответ на событие и выбора реакции на него уже реализованы в современных системах видеоаналитики, в том числе российских [4], но эффективная работа систем в огромной степени зависит от конкретного объекта наблюдения, условий съемки, наличия помех в области съемки. Не все моменты учитываются в системе правил, и это влияет на качество выбора реакции при срабатывании условия в правиле. Также необходимо применять систему правил для управления объемом хранилища видеоданных в зависимости от их важности, настройками камеры, адаптируя тем самым алгоритм работы системы мониторинга и анализа.

Многие системы ситуационной аналитики отличаются большим количеством ложных срабатываний, что в конечном итоге приводит к отключению части правил администраторами таких систем и, в конечном итоге, пропуску реальных событий. Проектирование системы автоматизированного обнаружения инцидентов – важная задача, решение которой связано с применением подходящих формализованных математических моделей, что не в полной мере освещено в современных публикациях. Системы нуждаются в изучении и усовершенствовании. Второй важной задачей является безопасная обработка данных видеонаблюдения, подпадающих под критерий «биометрические персональные данные», защита которых ужесточается [5].

Анализ опыта внедрения видеоаналитики в России и в мире

Одной из первых сфер применения видеоаналитики была транспортная безопасность. Особенностью применения видеоаналитики в транспортной сфере, согласно постановлению Правительства РФ № 969 2 «О сертификации технических средств транспортной безопасности», является требование сертификата соответствия для таких модулей, как

идентификация, стерильная зона (отсутствие людей), оставленный предмет, движение в запрещенном направлении, нетипичные изменения в картинке (затемнение, расфокусировка, засветка) [6].

Согласно прогнозу информационно-аналитического агентства TelecomDaily, в конце 2022 г. объем российского рынка видеоаналитики должен был достичь 12,8 млрд руб., что соответствует росту в среднем на 6 % ежегодно. Основные игроки в видеоаналитике: ГК ЦРТ (9 % рынка), NtechLab (8 %), Trassir/DSSL (7 %) и ITV/Axxon Soft (7 %) [7].

Популярная платформа TRASSIR включает технологию мгновенного поиска в архиве, систему «теплового» анализа (наложение цветовой шкалы на видео) активности в кадре, детекторы огня, дыма и саботажа. Базовый комплект можно дополнить модулем распознавания государственных регистрационных знаков автомобилей, трекинговым детектором SIMT, роботизированной функцией управления скоростными поворотными камерами, системой автоматического контроля и учета кассовых операций и другими модулями. Сделать систему безопасности еще более интеллектуальной и многоуровневой можно посредством интеграции программного обеспечения TRASSIR с системой контроля управления доступом и рядом других устройств.

С помощью интеллектуального детектора SIMT (Simple Intelligent Motion Trassir) можно выделить на видео объект, обладающий заданными параметрами, при этом на фоне допускается наличие многочисленного случайного движения, в большинстве случаев являющегося шумом. Детектор SIMT фильтрует сильные шумы, такие как качание веток деревьев, снег с дождем, легкие дрожания камеры и позволяет выделить на изображении реально движущиеся объекты. Объект, кратковременно скрывшийся из поля зрения (например, за деревом), не будет принят за новый или другой объект [8].

Можно настраивать параметры «Размер объекта в кадре», «Чувствительность», влияющие на результат обнаружения события, например во время контроля рабочего места. Так, чтобы неподвижный человек не воспринимался детектором как отсутствие человека на рабочем месте, задают значение параметру «Период остывания». Для повышения качества распознавания настраивают параметр «Место установки камеры: правильно/неправильно», который зависит от параметров «Размер объекта / размер всего кадра», «Помехи в области съемки» (например, открывающиеся двери в области съемки).

Недавно был принят первый национальный стандарт ГОСТ Р 59385-2021 «Информационные технологии. Искусственный интеллект. Ситуационная видеоаналитика. Термины и определения в области искусственного интеллекта для ситуационной видеоаналитики». Его принятие способствует упорядочиванию нормативного регулирования в этой области, которое только развивается. В данном документе даются базовые определения и представлены определения таких понятий, как сцена видеонаблюдения, свойства объекта сцены видеонаблюдения, ситуация, сценарий ситуации, класс, ситуационная и предиктивная видеоаналитика и др.

Но государственное регулирование может стать как драйвером, так и ограничителем рынка. Такие документы, как ФЗ-152 «О персональных данных» и ФЗ-149 «Об информации, информационных технологиях и о защите информации», существенно осложняют применение видеоаналитики, в особенности систем идентификации и верификации как для вендоров, так и для конечных пользователей. Биометрическая видеоаналитика применяется для идентификации и сопровождения лиц по биометрическим признакам лица.

Многие граждане с недоверием относятся к использованию систем видеоаналитики, опасаясь за свои права. Известно, что в Соединенных Штатах для повышения безопасности в городах запущена программа «нательных» камер у полицейских, в то же время суд в Балтиморе признал программу аэронаблюдения антиконституционной, приравняв ее к обыску без санкций. В 2021 г. Стокгольмскую транспортную организацию оштрафовали на 16 млн шведских крон за использование инспекторами носимых камер, отсутствие информирования граждан об этом и продолжительную видеозапись, в которой не было необходимости. Данные, которые обрабатываются в системах наблюдения, относятся к персональным данным и должны защищаться в соответствии с регламентом ЕС GDPR [9–12].

В разных странах стремятся урегулировать законодательство и технологию распознавания лиц для исключения возможности ею злоупотреблять. Для этого разрабатывают политики по использованию распознавания лиц, где описывают, в каких случаях применяется распознавание и идентификация человека (митинги, другие места наблюдения), какова процедура, как верифицируются совпадения, меры безопасности и ограничения доступа в систему, политика сохранения данных, в каких случаях другие организации и лица могут получить доступ к технологии и пр.

Данные видеоархива также должны очищаться по мере достижения целей обработки информации, так, в Амстердаме полиция обязана удалять из базы фотографии людей, которые более не являются подозреваемыми [10–12]. Таким образом, при проектировании систем событийного мониторинга для анализа видеоданных необходимо продумывать вопросы защиты личных данных и заранее включать в функционал специальные возможности для этого при технической реализации проектов, в част-

ности, удаление образа из базы шаблонов в случае достижения цели обработки, шифрование информации и ограничение доступа к ней при передаче, формирование уведомления граждан об использовании персональных данных.

Возможности и недостатки современных систем видеоаналитики

Системы событийного мониторинга могут объединять в своем составе различные сенсоры и модули: микрофоны, радиоволновые и вибрационные извещатели, модули аудио- и видеоаналитики.

Видеоаналитика, по сравнению с классическими средствами охраны, позволяет на более ранних стадиях обнаружить объект, причем на дальнем рубеже, назначить приоритет целям в зависимости от расстояния и вовремя среагировать на угрозу [13]. Хорошая видеоаналитика позволяет выделить наиболее важные фрагменты видео и удалять фрагменты, не представляющие интереса.

Современные камеры могут использовать программное обеспечение искусственного интеллекта, которое учитывает местоположение, время и модели поведения объектов для прогнозирования вероятности совершения нарушения.

Задачи видеоаналитики включают процесс обнаружения (установление факта появления объекта в зоне наблюдения), распознавания объекта или явления (определение типа наблюдаемого объекта – транспортное средство, человек, сумка, телефон, огонь, дым), идентификации объектов или явлений (сравнение свойств объекта с имеющимся образцом для установления соответствия (машина конкретного клиента, сотрудник компании, животное определенного вида или породы, класс опасности пожара)). Сравнение типов видеоаналитики представлено в табл. 1.

Таблица 1

Table 1

Типы видеоаналитики

Types of video analytics

Базовый	Расширенный	Искусственный интеллект или видеоаналитика с глубоким обучением
Для выявления событий (обнаружения движения) алгоритмы используют изменение пикселей, изменение цвета группы пикселей на изображении. Основной недостаток – количество ложных срабатываний, особенно в сложных сценах (при наличии тени, деревьев, изменении погодных условий и пр.)	Системы в анализе используют большие бинарные объекты, которые представляют собой группу связанных пикселей для поиска форм, что снижает количество ложных срабатываний.	Для анализа видеоматериалов используется нейронная сеть для обучения системы, точность обнаружения которой растет пропорционально числу изученных событий в процессе обучения. Процесс обучения может быть ручным (вмешательство человека для отметки соответствующих событий) или автоматическим, с использованием библиотек событий. Аналитика с глубоким обучением обеспечивает более продвинутый анализ – поиск функций, множественные условия, что позволяет быстрее и качественнее проводить анализ и сопоставление.

На данный момент самые незначительные успехи видеоаналитики – в решении задач распознавания ситуаций, поведения человека. Хорошие результаты наблюдаются в детектировании движения, оставленных предметов, а также при определенных «идеальных условиях» в трекинге движения отдельных объектов (но не в толпе). Многокамерный трекинг и классификация объектов при изменении ракурса по сравнению с вышеописанными задачами показывают слабые результаты [14].

Многокамерная или многоканальная видеоаналитика – технология, анализирующая поточное видео с разных камер, с учетом их расположения и данных, поступающих с сенсоров другого физического принципа (например, тепловизоров или радаров). В отличие от «однокамерной» видеоаналитики этот подход выявляет взаимосвязи между наблюдениями отдельных камер или сенсоров другого физического принципа, производит непрерывное слежение за каждым объектом при помощи всех доступных камер и сенсоров, построение обобщенной траектории его движения и автоматическое устранение избыточности данных в зонах перекрытия камер [14].

Алгоритмы настройки системы анализа видеоданных

Как известно, на плохих данных невозможно получить качественный анализ, поэтому данные перед обработкой надо «очистить». Чаще всего предварительная обработка используется для уменьшения

сложности обработки и повышения точности применяемого алгоритма.

Выделим некоторые виды предобработки, которые целесообразно выполнять для изображения, т. к. входные данные обычно поступают из разных источников:

– бинаризация;

– смена цветового пространства или приведение к оттенкам серого;

– удаление шумов;

– коррекция яркости и контраста изображений;

– сегментация.

На практике могут встречаться достаточно сложные локации для задач обнаружения и распознавания. Примером может служить локация, представленная на рис. 1.

Рис. 1. Выделение границы помещения

Fig. 1. Selection of the room boundary

С точки зрения области интересов следует проводить обнаружение и фиксировать объекты только внутри помещения, однако из-за того, что в помещении есть стеклянные стены, детектор будет обнаруживать еще и объекты снаружи. Также возможны ложноположительные срабатывания на отражение.

Контролируемые зоны можно ранжировать по сложности локации. При наличии таких зон следует определить границу, относительно которой объект будет либо внутри, либо снаружи. В процессе проведения эксперимента для настройки работы алгоритмов распознавания выделена горизонтальная граница, отделяющая пол и стеклянные стены (см. рис. 1).

Для каждого обнаруженного объекта детектор получает ограничивающую рамку, имея ее координаты, необходимо проверить пересечение условной границы. Если рамка пересекает линию или находится ниже, то объект находится внутри помещения и его появление необходимо фиксировать в журнале.

В ходе проведения эксперимента построена диаграмма распределения показателей точности принадлежности объектов к классу «Человек» до введения границы помещения (рис. 2).

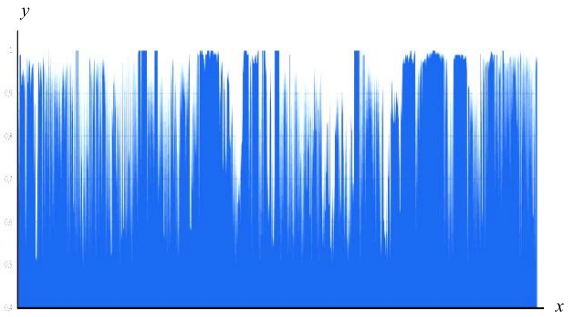

Рис. 2. Диаграмма распределения показателей точности до выделения границ помещения

Fig. 2. Diagram of the distribution of accuracy indicators before the selection of the room boundaries

На диаграмме видно, что значения показателей нестабильны, т. к. возможны срабатывания на отражения и отдаленные объекты. Благодаря выделению области интересов на второй диаграмме (рис. 3) распредление стало более стаблильным.

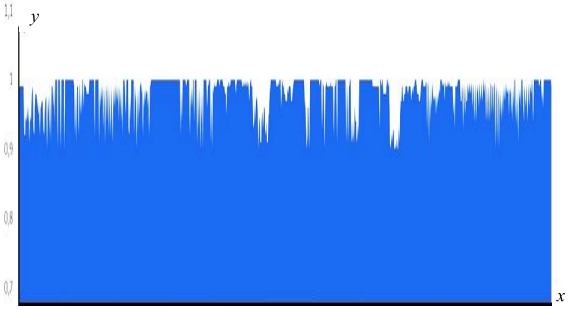

Рис. 3. Диаграмма распределения показателей точности после выделения границ помещения

Fig. 3. Diagram of the distribution of accuracy indicators after the selection of the room boundaries

После выделения границ помещения детектором фиксируются только объекты, которые находятся внутри помещения, т. е. они расположены достаточно близко к камере, чтобы вероятность обнаружения и распознавания была высокой, также были исключены ложноположительные срабатывания на отражения людей. Исходя из диаграммы, можно утверждать, что значение показателя достоверности наблюдается не ниже 90 %.

Данный инструмент можно использовать в качестве детектора пересечения границы для защищенных помещений или для подсчета количества людей, которые зашли в помещение.

Проектирование системы правил для организации мониторинга

Принцип действия видеоаналитики – выявление отклонений. Разработчики применяют нейросетевой

подход и машинное обучение для обнаружения отклонений с помощью распространенных библиотек-детекторов – саботаж, движение, появление объекта в зоне и др. Для управления событиями, реакцией на них применяется система правил. Рассмотрим на рис. 4 возможности создания правил в системе TRASSIR на примере создания правила в связи с изменением состояния сигнала с камер, установленных в зоне наблюдения склада [15].

Рис. 4. Создание правила в системе TRASSIR

Fig. 4. Creating a rule in the TRASSIR system

Любое правило состоит из активации и действия, статистика срабатывания и появления которых учитывается в соответствии с алгоритмом работы. Активация – это событие, при возникновении которого запускается правило. Пример правила: если объект в кадре – животное, и оно небольшое, то это «разрешенный» объект (не значимый), реакции нет. Так, например, обнаруженный и распознанный предмет в кадре может считаться допустимым или нет в зависимости от заданного размера, месторасположения, времени обнаружения или длительности нахождения в кадре.

Правила – это простой способ настройки сценариев работы системы типа «событие → реакция». Пользователь выбирает из имеющихся списков события, условия, указывает действия, которые должна выполнить программа.

В современных системах видеоаналитики могут реализовываться скрипты для создания различных сценариев моделирования реакции в ответ на событие. Для написания скриптов в TRASSIR требуются квалификация в области программирования и знание Python [8, 15].

Пример скрипта.

Активация по событию AutoTRASSIR:

```
def f(ev):
message(«Проехала машина с номером %s» % ev.plate)
activate_on_lpr_events(f)
```

В TRASSIR можно настроить также срабатывание тревоги только на людей или только на транспортное средство, что позволит оператору сосредоточиться на особых угрозах и не пропустить реальную тревогу, при этом дальнейшая идентификация незначимого события не требуется, фрагмент с изображением можно удалить.

Ложным сигналам тревоги наиболее подвержены периметры объектов, где детекторы движения видеокамер реагируют на дождь или снег, качающиеся ветки деревьев и пр.

Таким образом, грамотный подбор камер видеонаблюдения, их правильная настройка, выбор количества зон распознавания и определение их границ также могут описываться системой правил посредством дополнительных скриптов или модулей. Для этого нужно задавать приоритеты, определяя значимые события, задавая приоритеты для них и несовместимость для отдельных сочетаний, например:

– одновременное нахождение в разных зонах одного и того же человека свидетельствует об ошибке распознавания;

– выход из зоны без регистрации входа в нее может свидетельствовать об изменении облика объекта для введения в заблуждение контролера;

– обнаружение в зоне человека, который долгое время не покидал зону в обратном направлении, свидетельствует о его перемещении, например, в обход системы контроля.

В процессе анализа данных мониторинга для обнаружения опасного инцидента требуется анализ связей между несколькими обнаруженными признаками. Чтобы выявить опасные инциденты, требующие реакции, нужно понимать, что является правилом.

Не всегда правило может быть получено в ходе обучения, т. к. правила могут устанавливаться политиками и регламентами информационной безопасности заранее, хотя могут меняться и уточняться позже, в том числе на основе использования данных видеоаналитики. В свою очередь, правила в алгоритмах работы детекторов также могут быть спорными (например, что считать нестандартным поведением, плохим изображением, или когда считать похожим / не очень похожим на человека объект из черного списка). В реальном времени может сработать сразу несколько правил, события фиксироваться несколькими камерами. В этом случае необходимо также предложить алгоритмы поведения и выбора варианта действия. Здесь могут помочь системы мониторинга на базе методов нечеткого управления, которые используют нечеткие данные и позволяют осуществлять управление, прогнозирование результата на основе большого числа правил.

Используемый в экспертных и управляющих системах механизм нечетких выводов в своей основе имеет базу знаний, формируемую специалистами предметной области в виде совокупности нечетких предикатных правил вида

IF < посылка 1 > *AND* < посылка 2 > … *AND* <
< посылка *n* > *THEN* < заключение >

IF < посылка 1 > *OR* < посылка 2 > … *OR* <
< посылка *n* > *THEN* < заключение >

Часть «*THEN*» может содержать несколько заключений, где каждому подзаключению сопоставлен еще и определенный весовой коэффициент *cf*:

$$cf = \frac{MB(H, E) - MD(H, E)}{1\text{-}\min[MB(H, E), MD(H, E)]},$$

где $MB(H, E)$ = мера доверия; $MD(H, E)$ – мера недоверия.

Факторы уверенности *cf* задаются экспертно для каждого из правил базы знаний экспертной системы:

IF < факт *E* > *THEN* < гипотеза *H* >:

Эти функции указывают, соответственно, степень увеличения доверия к гипотезе *H*, если факт *E* произошел, и степень увеличения недоверия к гипотезе *H*, если факт *E* имел место.

Формализовать политики, правила реагирования на событие удобно с применением системы нечеткого вывода, где параметрами модели могут являться данные как из системы видеонаблюдения, так и из альтернативных источников (системы DLP, описательные данные из социальных сетей, полученные об объекте в режиме реального времени).

Примеры параметров модели – место съемки (известное, популярное, социально значимое), время съемки (раннее, позднее, рабочее, ночное), возраст человека (молодой, пожилой), поведение (агрессивное, подозрительное, нестандартное), количество людей (большое, среднее, малое) и т. д.

Пусть *X* – множество политик (правил); *Y* – множество лингвистических входных переменных (например, время, место наступления события, размер объекта, сходство объекта наблюдения и др.); *Z* – множество лингвистических выходных переменных (скорость реакции, вероятность инцидента, степень риска). Правила можно формализовать в виде

П1: Если Время наступления события = позднее
И Место = социально значимое
И Поведение = агрессивное,
То Риск нарушения = средний.

П2: Если Время наступления события = нерабочее
И Место = запрещенное
И Поведение = подозрительное,
Схожесть объекта
с доверенным пользователем системы = низкая,
То Риск нарушения = высокий.

Для задания связи вероятности инцидента с реакцией на него можно получить данные от экспертов и составить таблицу реагирования (табл. 2).

Таблица 2

Table 2

Правила реагирования

Rules of response

Вероятность инцидента		
низкая	**средняя**	**высокая**
Запись с камер предоставить оператору для оценки	Запись с камер предоставить оператору, записать данные в БД с необходимыми атрибутами	Запись с камер предоставить оператору для внесения в БД и отправить коптер (БПЛА) к месту происшествия

Также при проектировании системы событийного мониторинга нужно учитывать, что часто алгоритмы отслеживания работают быстрее алгоритмов обнаружения.

При отслеживании объекта, который был обнаружен в предыдущем кадре, можно применять данные о внешнем виде объекта, взятые из предыдущего кадра. Идентификация субъекта может быть реализована с применением «безликого распознавания», когда такие физические характеристики, как рост, осанка и телосложение, используются для идентификации человека в толпе. Также могут быть известны местоположение в предыдущем кадре, направление и скорость движения объекта. Соответственно, можно использовать всю эту информацию, чтобы предсказать местоположение объекта в следующем кадре и выполнить поиск в месте ожидаемого местоположения объекта [16]. Отслеживание, как правило, более устойчиво к окклюзиям, когда отслеживаемый объект частично скрыт или полностью перекрыт другим объектом, что мешает обнаружению. Хороший алгоритм отслеживания может просчитать возможные места появления объекта, хотя есть эффект накопления ошибок. На рис. 5 представлена блок-схема алгоритма анализа видеоданных на основе распределения зон наблюдения по степени важности.

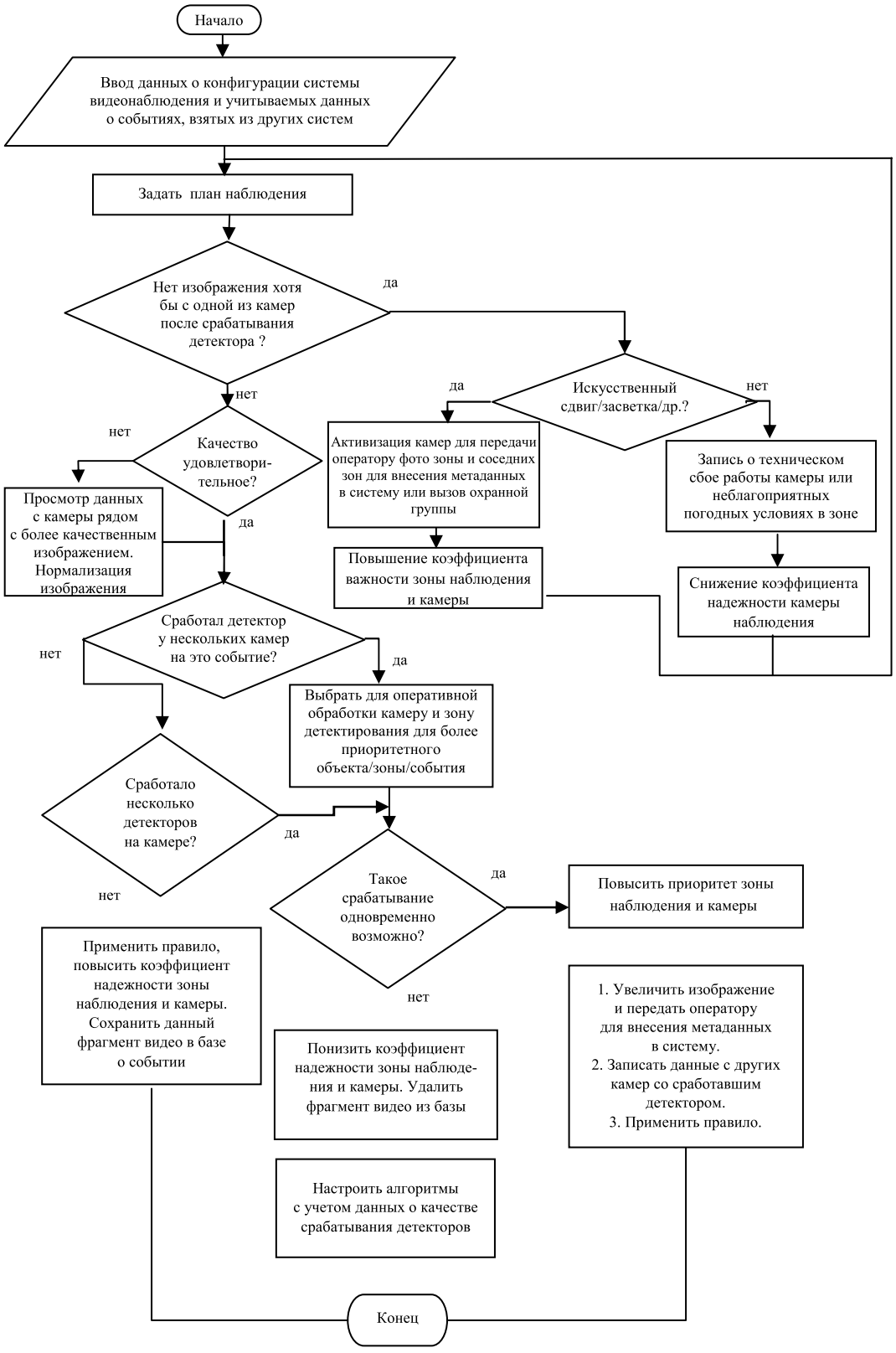

Рис. 5. Блок-схема алгоритма анализа видеоданных

Fig. 5. Graph of the algorithm of video data analysis

Ввод данных о конфигурации системы наблюдения подразумевает указание количества камер, их характеристик, мест установки, их связи с зонами наблюдения, задание приоритетов зонам наблюдения, событиям, а также указание данных о собираемых атрибутах в процессе ведения журналов аудита системами СКУД, ОС, DLP и др.

Построение плана наблюдения подразумевает задание параметров работы алгоритмов, правил выбора действий системы на случай одновременного срабатывания детекторов и т. д. Так, выбор приоритетного объекта может базироваться на расчетных критериях: расстоянии до камеры, качестве изображения с учетом шумов, помех (погода, тени, пересечение с другими объектами, засветка камеры стеклянными объектами, уровень освещения и т. д.), расстоянии до рубежа защиты, возможности создания преграды на пути объекта к рубежу защиты и др.

Заключение

Технология распознавания изображений активно применяется в системах событийного мониторинга.

Выявлены важные обязательные этапы в процессе проектирования современных систем событийного мониторинга, определены узкие места, предложены модели решения.

Путем эксперимента были выявлены обязательные этапы предварительной обработки изображений для повышения уровня распознавания, в рамках эксперимента была протестирована методика выравнивания гистограммы для обработки яркости и контрастности изображения.

Данные, которые собирает и обрабатывает система событийного мониторинга, должны быть в безопасности, чтобы сохранить конфиденциальность пользователей и компании. Обзор проблем и их решений по данному вопросу также представлен в исследовании.

Список источников

1. Митягина М. И., Лаврова О. Ю., Бочарова Т. Ю. Спутниковый мониторинг нефтяных загрязнений морской поверхности // Современные проблемы дистанционного зондирования Земли из космоса. 2015. Т. 12, № 5. С. 130–149.

2. Василий_Долгов,_генеральный_директор_VizorLabs: Что_должна_уметь_современная_платформа_видеоаналитики? URL: https://news.myseldon.com/ru/news/index/287318908 (дата обращения: 21.01.2023).

3. Проблемы и перспективы видеоаналитики. URL: https://www.secuteck.ru/articles/problemy-i-perspektivy-video analitiki (дата обращения: 21.01.2023).

4. Терминалы и интегрированные системы контроля доступа с биометрическим распознаванием лиц. URL: http://www.techportal.ru/review/sistemy-kontrolya-do stupa-s-raspoznavaniem-lits (дата обращения: 23.01.2023).

5. Разъяснения к Федеральному закону о внесении изменений в ФЗ «О персональных данных» (№ 266 от 14.07.2022). URL: https://www.anti-malware.ru/analytics/Technology_Analysis/President-Decree-266-Clarifications (дата обращения: 20.01.2023).

6. Проблемы и перспективы видеоаналитики. URL: https://www.drdoors-msc.ru/stati/problemy-i-perspektivy-videoanalitiki.html (дата обращения: 26.01.2023).

7. «Рынок продолжает оставаться разрозненным»: экспертный прогноз развития рынка видеоаналитики до 2023 года. URL: https://new-retail.ru/tehnologii/rynok_prodolzhaet_ostavatsya_razroznennym_ekspertnyy_prognoz_razvitiya_rynka_videoanalitiki_do_2023_7344/ (дата обращения: 02.02.2023).

8. TRASSIR. Руководство администратора. URL: https://chileruschool.ru/45/a8f42be32077c552faf7d24ea2499808.pdf (дата обращения: 27.01.2023).

9. Azarov V. G., Chuprina M. V. The possibilities of biometric video analytics and the rules of its application // Economics. Information technologies. 2022. N. 49 (1). P. 169–177.

10. GDPR DAY для бизнеса 2023. URL: https://ogdpr.eu/ru (дата обращения: 18.01.2023).

11. Видеонаблюдение и видеоаналитика. Исследование зарубежного опыта. URL: https://ict.moscow/static/74aa34ad-13a5-5f3e-816f-aaf1e883da61.pdf (дата обращения: 27.01.2023).

12. Амельчакова В. Н., Суслова Г. Н. Использование сотрудниками полиции систем видеорегистрации (международный опыт) // Вестн. эконом. безопасности. 2018. № 4. С. 140–144. URL: https://cyberleninka.ru/article/n/ispolzovanie-sotrudnikami-politsii-sistem-videoregistratsii-mezhdunarodnyy-opyt (дата обращения: 17.01.2023).

13. Птицын Н. Видеоанализ в системах защиты периметра. URL: http://habrahabr.ru/company/synesis/blog/137006/ (дата обращения: 03.02.2023).

14. Свиридов В. П., Сбродов В. В., Лазарев Н. Ю., Лазарев Ю. Н. Мультисенсорная система измерения угловой ориентации космического аппарата относительно подстилающей поверхности // Вестн. компьютер. и информац. технологий. 2016. № 6 (144). С. 18–26. URL: http://elibrary.ru/item.asp?id=26366687 (дата обращения: 15.02.2023).

15. Техническая документация для ПО TRASSIR. URL: https://www.dssl.ru/support/tech/documentation/potrassir/ (дата обращения: 09.02.2023).

16. Ямшанов К. Л., Киселев А. О., Легкий В. Н., Гибин И. С. Навигация малых БПЛА на основе видеосистем // Наука. Промышленность. Оборона – 2019: тр. XX Всерос. науч.-техн. конф., посвящ. 150-летию со дня рождения С. А. Чаплыгина: в 4 т. (Новосибирск, 17–19 апреля 2019 г.). Новосибирск: Изд-во Новосиб. ГТУ, 2019. Т. 2. С. 386–391.

References

1. Mitiagina M. I., Lavrova O. Iu., Bocharova T. Iu. Sputnikovyi monitoring neftianykh zagriaznenii morskoi poverkhnosti [Satellite monitoring of oil pollution of sea surface]. *Sovremennye problemy distantsionnogo zondirovaniia Zemli iz kosmosa*, 2015, vol. 12, no. 5, pp. 130-149.

2. *Vasilii Dolgov, general'nyi director VizorLabs: Chto dolzhna umet' sovremennaia platform videoanalitiki* [General director of VizorLabs Vasily Dolgov: what a modern video analytics platform should be able to do]. Available at: https://news.myseldon.com/ru/news/index/287318908 (accessed: 21.01.2023).

3. *Problemy i perspektivy videoanalitiki* [Problems and prospects of video analytics]. Available at: https://www.secuteck.ru/articles/problemy-i-perspektivy-videoanalitiki (accessed: 21.01.2023).

4. *Terminaly i integrirovannye sistemy kontrolia dostupa s biometricheskim raspoznavaniem lits* [Terminals and integrated access control systems with biometric face recognition]. Available at: http://www.techportal.ru/review/sistemy-kontrolya-do stupa-s-raspoznavaniem-lits (accessed: 23.01.2023).

5. *Raz"iasneniia k Federal'nomu zakonu o vnesenii izmenenii v FZ «O personal'nykh dannykh» (№ 266 ot 14.07.2022)* [Clarifications to the Federal Law on Amendments to the Federal Law “On Personal Data” (No. 266 of July 14, 2022)]. Available at: https://www.anti-malware.ru/analytics/Technology_Analysis/President-Decree-266-Clarifications (accessed: 20.01.2023).

6. *Problemy i perspektivy videoanalitiki* [Problems and prospects of video analytics]. Available at: https://www.drdoors-msc.ru/stati/problemy-i-perspektivy-videoanalitiki.html (accessed: 26.01.2023).

7. *«Rynok prodolzhaet ostavat'sia razroznennym»: ekspertnyi prognoz razvitiia rynka videoanalitiki do 2023 goda* [Market remains fragmented: expert forecast development of video analytics market until 2023]. Available at: https://new-retail.ru/tehnologii/rynok_prodolzhaet_ostavatsya_razroznennym_ekspertnyy_prognoz_razvitiya_rynka_videoanalitiki_do_2023_7344/ (accessed: 02.02.2023).

8. *TRASSIR. Rukovodstvo administratora* [TRASSIR. Administrator’s guide]. Available at: https://chileruschool.ru/45/a8f42be32077c552faf7d24ea2499808.pdf (accessed: 27.01.2023).

9. Azarov V. G., Chuprina M. V. The possibilities of biometric video analytics and the rules of its application. *Economics. Information technologies*, 2022, no. 49 (1), pp. 169-177.

10. *GDPR DAY dlia biznesa 2023* [GDPR DAY for business 2023]. Available at: https://ogdpr.eu/ru (accessed: 18.01.2023).

11. *Videonabliudenie i videoanalitika. Issledovanie zarubezhnogo opyta* [Video surveillance and video analytics. Study of foreign experience]. Available at: https://ict.moscow/static/74aa34ad-13a5-5f3e-816f-aaf1e883da61.pdf (accessed: 27.01.2023).

12. Amel'chakova V. N., Suslova G. N. Ispol'zovanie sotrudnikami politsii sistem videoregistratsii (mezhdunarodnyi opyt) [Use of video recording systems by police officers (international experience)]. *Vestnik ekonomicheskoi bezopasnosti*, 2018, no. 4, pp. 140-144. Available at: https://cyberleninka.ru/article/n/ispolzovanie-sotrudnikami-politsii-sistem-videoregistratsii-mezhdunarodnyy-opyt (accessed: 17.01.2023).

13. Ptitsyn N. *Videoanaliz v sistemakh zashchity perimetra* [Video analysis in perimeter protection systems]. Available at: http://habrahabr.ru/company/synesis/blog/137006/ (accessed: 03.02.2023).

14. Sviridov V. P., Sbrodov V. V., Lazarev N. Iu., Lazarev Iu. N. Mul'tisensornaia sistema izmereniia uglovoi orientatsii kosmicheskogo apparata otnositel'no podstilaiushchei poverkhnosti [Multisensor system for measuring angular orientation of spacecraft relative to underlying surface]. *Vestnik komp'iuternykh i informatsionnykh tekhnologii*, 2016, no. 6 (144), pp. 18-26. Available at: http://elibrary.ru/item.asp?id=26366687 (accessed: 15.02.2023).

15. *Tekhnicheskaia dokumentatsiia dlia PO TRASSIR* [Technical documentation for TRASSIR software]. Available at: https://www.dssl.ru/support/tech/documentation/potrassir/ (accessed: 09.02.2023).

16. Iamshanov K. L., Kiselev A. O., Legkii V. N., Gibin I. S. Navigatsiia malykh BPLA na osnove videosistem [Navigation of small UAVs based on video systems]. *Nauka. Promyshlennost'. Oborona – 2019: trudy XX Vserossiiskoi nauchno-tekhnicheskoi konferentsii, posviashchennoi 150-letiiu so dnia rozhdeniia S. A. Chaplygina: v 4 t. (Novosibirsk, 17–19 aprelia 2019 g.).* Novosibirsk, Izd-vo Novosib. GTU, 2019. Vol. 2. Pp. 386-391.

Статья поступила в редакцию 26.03.2023; одобрена после рецензирования 26.04.2023; принята к публикации 07.07.2023
The article was submitted 26.03.2023; approved after reviewing 26.04.2023; accepted for publication 07.07.2023

Информация об авторах / Information about the authors

Ирина Михайловна Космачева – кандидат технических наук, доцент; доцент кафедры информационной безопасности; Астраханский государственный технический университет; ikosmacheva@mail.ru

Irina M. Kosmacheva – Candidate of Technical Sciences, Assistant Professor; Assistant Professor of the Department of Information Security; Astrakhan State Technical University; ikosmacheva@mail.ru

Иван Юрьевич Кучин – кандидат технических наук; доцент кафедры информационной безопасности; Астраханский государственный технический университет; kuchin@astu.org

Надежда Валерьевна Давидюк – кандидат технических наук, доцент; доцент кафедры информационной безопасности; Астраханский государственный технический университет; davidyuknv@bk.ru

Михаил Федорович Руденко – доктор технических наук, профессор; профессор кафедры безопасности жизнедеятельности и инженерной экологии; Астраханский государственный технический университет; mf.rudenko@mail.ru

Владимир Иванович Лобейко – доктор технических наук, профессор; профессор кафедры высшей математики и информатики; Астраханский государственный технический университет; lobeykov@mail.ru

Ирина Вячеславовна Сибикина – кандидат технических наук, доцент; доцент кафедры информационной безопасности; Астраханский государственный технический университет; isibikina@bk.ru

Ivan Yu. Kuchin – Candidate of Technical Sciences; Assistant Professor of the Department of Information Security; Astrakhan State Technical University; kuchin@astu.org

Nadezda V. Davidyk – Candidate of Technical Sciences, Assistant Professor; Assistant Professor of the Department of Information Security; Astrakhan State Technical University; davidyuknv@bk.ru

Mikhail F. Rudenko – Doctor of Technical Sciences, Professor; Professor of the Department of Life Safety and Engineering Ecology; Astrakhan State Technical University; mf.rudenko@mail.ru

Vladimir I. Lobeyko – Doctor of Technical Sciences, Professor; Professor of the Department of Higher Mathematics and Computer Science; Astrakhan State Technical University; lobeykov@mail.ru

Irina V. Sibikina – Candidate of Technical Sciences, Assistant Professor; Assistant Professor of the Department of Information Security; Astrakhan State Technical University; isibikina@bk.ru