

Проектирование системы видеоаналитики нарушений требований промышленной безопасности на площадках сооружения АЭС

А. Ю. Исакова, В. И. Шармаев

Аннотация — Строительная площадка – это объект повышенной зоны риска для всех, кто находится на ней, поэтому меры обеспечения безопасности, предъявляемые данной территории, должны соблюдаться неукоснительно. Зачастую процесс соблюдения техники безопасности носит формальный характер и заключается в проведении периодических инструктажей и тренировок персонала, а функция непосредственного контроля, как правило, закреплена за непосредственными начальниками. Технологии видеоаналитики и обработки изображений позволяют минимизировать эти затраты и повысить уровень безопасности, своевременно предупреждая о возможных нарушениях в работе людей или машин. Видеоаналитика — это постоянно развивающаяся область, в которой постоянно разрабатываются новые методы и алгоритмы в таких областях, как семантическая категоризация видео, извлечение видео из базы данных, распознавание действий человека, обобщение и обнаружение аномалий. Статья посвящена разработке требований к системе и архитектуре информационной системы строительного контроля как части концептуальной модели. Авторами было исследовано текущее состояние в организации с точки зрения автоматизации, проанализирована проблема и возможные решения, разработаны требования к функциям системы, описаны требования к инфраструктуре, разработан прототип решения. Внедрение системы видеоаналитики нарушений требований техники безопасности позволит повысить эффективность деятельности по обеспечению безопасности за счет снижения травматизма работников при производстве работ, а также за счет повышения трудовой дисциплины и культуры безопасности.

Статья получена 28 июня 2022. Работа представляет собой результат магистерской диссертации Исаковой Анастасии Юрьевны на тему «Анализ и разработка требований к системе видеоаналитики нарушений требований промышленной безопасности на площадках сооружения АЭС».

Исакова Анастасия Юрьевна – магистр Национального исследовательского ядерного университета «МИФИ» (e-mail: nastasja.isakova98@gmail.com).

Шармаев Вадим Игоревич – аспирант ФГБОУ ВО «Московский авиационный институт (национальный исследовательский университет)» (e-mail: vadssx@ya.ru).

Ключевые слова — система видеоаналитики, техника безопасности, архитектура системы, фиксация нарушений, анализ инцидентов.

I. ВВЕДЕНИЕ

На производствах с высокой травмоопасностью, в том числе в строительной отрасли, соблюдать технику безопасности всегда было жизненно важно и необходимо. Строительная площадка – это объект повышенной зоны риска для всех, кто находится на ней, поэтому меры обеспечения безопасности, предъявляемые к данной территории, должны соблюдаться неукоснительно. При кадровом аудите зачастую выясняется, что в компании попросту отсутствуют специалисты по технике безопасности, а также инструкторы, прошедшие обучение охране труда и допущенные к инструктажам работников [1]. Техника безопасности и охрана труда предполагают систему периодических инструктажей, обучение работников, а также проверку их знаний. Если работник такую проверку знаний не проходит либо систематически нарушает или не исполняет правила, работодатель вправе временно отстранить его от работы или применить иные способы борьбы с несоблюдением сотрудником правил безопасности: выговор, лишение премии, прекращение трудового договора [2].

Зачастую процесс соблюдения техники безопасности носит формальный характер и заключается в проведении периодических инструктажей и тренировок персонала, а функция непосредственного контроля, как правило, закреплена за непосредственными начальниками (бригадиром, мастером, начальником смены и т.д.) [3].

Самыми частыми причинами несчастных случаев на производстве являются неудовлетворительная организация производства работ, нарушение технологического процесса, нарушение работником трудового распорядка и дисциплины труда, недостатки в подготовке работников по охране труда, эксплуатация неисправных механизмов и оборудования и нарушение требований охраны труда при эксплуатации транспортных средств [4].

Нарушение техники безопасности приводит не только к травмам и смертельным случаям, но и к прямым убыткам компаний работодателей, которые определяются различного рода простоями, выходом из рабочего состояния оборудования или нарушением

технологического процесса, а, в следствии, снижением инвестиционной привлекательности компании. Бизнес-процесс по контролю техники безопасности может быть организован путем внедрения систем автоматизированного видеонализа в рамках данного бизнес-процесса [5]. Дополнительно к вышесказанному стоит отметить, что непосредственные участники процесса обеспечения безопасности на площадке строительства АЭС сталкиваются с множеством технических проблем, например, при формировании отчетов по выявленным нарушениям за отчетный период. Отсутствие инструментов мониторинга и анализа нарушений техники безопасности не позволяют в полной мере обеспечить безопасность при выполнении работ и контролировать ношение средств индивидуальной защиты персоналом.

II. ЛИТЕРАТУРНЫЙ ОБЗОР

Большое количество случаев травматизма на предприятии и частые простои из-за несчастных случаев негативно сказываются не только на прибыли компании, но и на ее имидже. Технологии видеоналитики и обработки изображений позволяют минимизировать эти затраты и повысить уровень безопасности, своевременно предупреждая о возможных нарушениях в работе людей или машин [6].

В целом, возможности таких систем могут быть разнообразны и не ограничиваться одним лишь предотвращением травматизма. Видеоналитика включает в себя не только мониторинг в целях безопасности или охраны, но и мониторинг для отслеживания различных процессов, например, розничной торговли, транспорта, сферы услуг и здравоохранения [7]. Видеоналитика — это постоянно развивающаяся область, в которой постоянно разрабатываются новые методы и алгоритмы в таких областях, как семантическая категоризация видео, извлечение видео из базы данных, распознавание действий человека, обобщение и обнаружение аномалий [8].

Спорт, розничная торговля, автомобилестроение, транспорт, безопасность, развлечения, управление дорожным движением, включая пешеходные переходы, цифровые устройства для принятия решений в реальном времени и здравоохранение — это лишь некоторые из нескольких областей, в которых применяется видеоналитика.

Из российских систем "Спецлаб-ЦАФАП" — это первая, которая контролирует на улицах городов широкий спектр нарушений ПДД и при этом обеспечивает оперативный мониторинг автотранспорта в реальном времени (Рисунок 1), позволяя пресекать нарушения в текущий момент, а не только после обработки полученного материала [9].

Avigilon, продукт Motorola Solutions, предлагает полный спектр продуктов безопасности, объединенных в единый высокотехнологичный пакет [10]. Благодаря использованию самообучающихся систем анализа достигается высокая производительность служб безопасности, а процесс мониторинга становится более экономичным и эффективным.



Рис. 1 – Интерфейс системы Спецлаб-ЦАФАП

Камеры Avigilon могут действовать как интеллектуальный детектор после определенного периода исследования сцены (Рисунок 2), передавая все нестандартные ситуации на сервер в отдельном потоке [11].

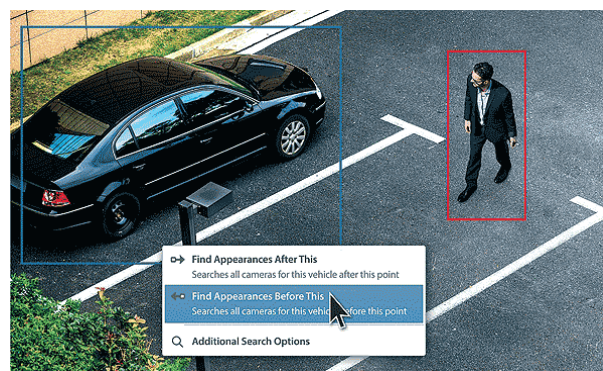


Рис. 2 – Система Avigilon

III. МАТЕРИАЛЫ И МЕТОДЫ

Для того, чтобы программный продукт был понятен пользователю необходимо несколько условий [12]. Во-первых, удобный и понятный интерфейс пользователя. Выбор параметров запроса или информации для анализа инцидентов должен происходить в диалоговом режиме. Во-вторых, формируемые отчеты для пользователя должны быть также понятны.

Очевидно, что, если пользователь нуждается в обработке большого потока данных, время ожидания не должно быть долгим.

Другим требованием является гибкость программного продукта. Гибкость в данном случае можно рассматривать как возможность выбора параметров вводимой информации и формируемых отчетов пользователем.

Так как создаваемый программный продукт будет обладать гибкостью, затраты на поддержку и сопровождение системы должны быть минимальны.

В рамках анализа ИТ-решений по видеоналитике рассматриваются только вендоры с ПО, зарегистрированным в едином реестре российских программ для электронных вычислительных машин и баз данных, а также решения, позволяющие реализовать сценарии видеонализа, которые могут быть применены

в производстве (например, Vizorlabs [13]).

Разрабатываемая система предназначена для выявления фактов нарушения правил применения средств индивидуальной защиты работниками предприятий; выявления нарушений работниками периметра опасных зон; сбора и хранения полученных данных; снижения травматизма персонала при производстве работ; создания системы компьютерного видеонализа соблюдения техники безопасности; повышения трудовой дисциплины.

Процесс автоматической фиксации нарушений требований техники безопасности работниками без участия оператора, включает в себя следующие этапы:

1. Работник появляется в зоне детектирования.
2. Модуль детектирования производит подсчет количества работников, находящихся в зоне детектирования.
3. Модуль идентификации событий нарушения ТБ выполняет проверку по следующим критериям:
 - каска – отсутствует или надета;
 - перчатки – отсутствуют одна или обе;
 - куртка – застегнута полностью или нет;
 - нарушение периметра опасной зоны – наличие или отсутствие персонала в опасной зоне;
 - медицинская маска – отсутствует или надета;
 - нарушение социальной дистанции;
4. При прохождении проверки процесс завершается.
5. Если проверка не пройдена, то в модуле обработки событий выполняется сопоставление индекса вероятности нарушения ТБ и ПБ.
6. При превышении допустимого значения в модуле обработки событий фиксируется факт нарушения и направляется уведомление оператору.
7. Если индекс ниже допустимого значения, то процесс завершается.
8. Сведения по факту нарушения должны быть сохранены в модуле хранения фотографий и видеофрагментов. После этого процесс завершается.

Аналогично был описан процесс нарушений периметра опасных зон работниками, процесс фиксации наличия спецтехники в зоне детектирования, процесс формирования и загрузки отчетности с помощью модуля запросов и формирования отчетов (Рисунок 3).

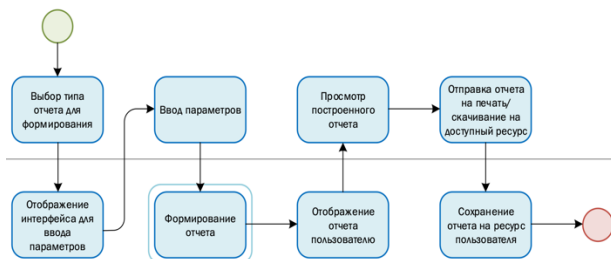


Рис. 3 – Схема процесса автоматической фиксации нарушений ТБ

IV. РЕЗУЛЬТАТЫ

Информация о нарушении, представленная в карточке нарушения, сопровождается в системе самим фрагментом нарушения, 5 секундами, предшествующих моменту детектирования нарушения, и 5 секундами после него.

В настройках системы также реализована возможность устанавливать глубину хранения данных о нарушениях (в днях), по достижении которой соответствующие данные должны автоматически удаляться из БД системы (информация о самом нарушении, файлы с фото и видео фрагментом нарушения) и в её интерфейсе больше не отображаться. Процедура очистки данных запускается периодически, интервал проверки (в секундах) также задаётся в интерфейсе системы.

Архитектура системы строится на принципе сервис-ориентированной архитектуры (COA), которая позволяет обеспечить модульный подход к разработке программного обеспечения [14], а также на основе трехзвенной архитектуры, которая включает базы данных, серверы приложений, «тонкие» и мобильные клиенты [15].

Основные компоненты архитектуры (Рисунок 4):

1. *Веб-клиент*, реализованный на базе React UI. Основной функционал: интерфейс на добавлении/редактирование камер, мониторинг работы системы, просмотра видеопотоков и видеопотоков, с наложенной визуализацией работы детекторов.

2. *БД* — база данных для хранения задач для манипулирования потоков, настроек камер и информации о событиях. Реализация на базе Postgres.

3. *Хранилище моделей* — репозиторий с возможностью версионного хранения обученных нейросетей для работы детекторов.

4. *Сервис авторизации* — подсистема аутентификации и авторизации пользователей, распределения прав и доступа к личным кабинетам.

5. *Сервис управления медиасerverами* — инструмент для запуска одноразовых/периодических задач, используется для запуска/остановки обработки видеопотоков, а также запускает задачи на переключение репозитория.

6. *Медиасервер* — сервис для передачи видеопотоков и кадров на обработку в детекторы и отображения видеопотоков и результатов работы нейронных сетей на этих потоках (видеопотоки с визуализацией). Представляет видеопотоки по технологиям Motion Jpeg, hls, rstp.

7. *Балансировщик* — система, при подключении или отключении камер и с заранее фиксированной периодичностью проводящая балансировку видеопотоков на презентованные сервера и GPU процессоры.

8. *Детекторы* — нейросети (модули видеоаналитики) и логика, необходимая для детектирования событий и нарушений на видеопотоках. Детектируемые инциденты нарушений включают в себя идентификацию наличия СИЗ, обнаружение падения человека, видеоконтроль нахождения в зоне, идентификация возгорания, идентификацию поднятой стрелы автокрана при движении

9. *Тепловая карта* — алгоритм определяет места с наиболее частым нахождения людей

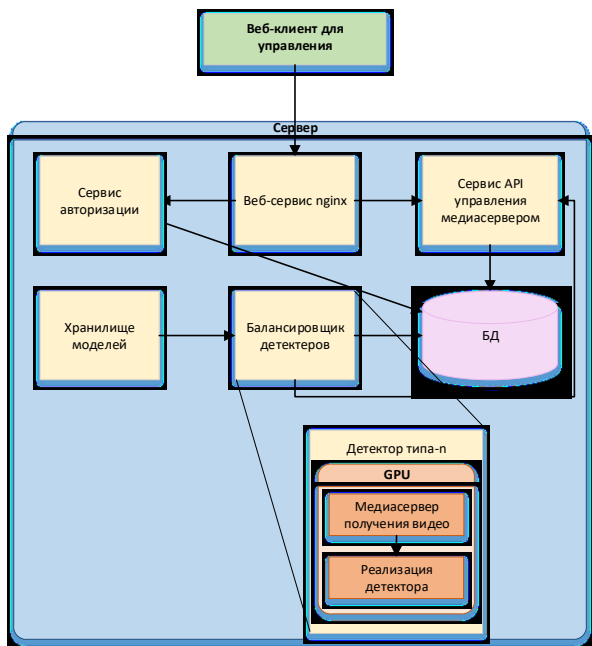


Рис. 4 - Взаимодействие между компонентами системы

V. ОБСУЖДЕНИЕ

Социальный эффект предложенной системы сосредоточен на использовании информационных технологий для улучшения условий и качества труда работников. Внедрение системы видеонализа в области охраны труда может снизить количество нарушений техники безопасности в 10 раз [16].

Алгоритм воздействия на сотрудника, не соблюдающего технику безопасности, в общем виде представляет собой следующие шаги:

1. При выявлении нарушения надо зафиксировать факт нарушения актом о несоблюдении правил техники безопасности.

2. На основе акта нужно истребовать у работника письменные объяснения, согласно ст. 193 ТК [17].

3. Непосредственный руководитель работника или сотрудник, ответственный за контроль соблюдения техники безопасности, составляет докладную записку на имя генерального директора с описанием ситуации, объяснений работника, причин, повлекших нарушение, тяжести нарушения, а также предложения, как наказать сотрудника и принять меры по пресечению повторных нарушений.

4. На основании всех этих документов принимается решение привлечь работника к ответственности (например, издать приказ о выговоре).

5. На основании этого приказа лишить работника права на премии в течение определенного времени.

Помимо описанных требований к системе, разрабатываемый продукт должен быть надежно защищен с точки зрения информационной безопасности.

Информационная безопасность — это защита данных от кражи или изменения, случайного или преднамеренного [18]. Система информационной безопасности организации является эффективным инструментом защиты интересов владельцев и пользователей информации [19]. Следует отметить, что

не только несанкционированный доступ к информации может нанести ущерб. Она может быть вызвана сбоем в работе средств связи или информации.

Для обеспечения защиты информации в системе используются следующие методы:

1. Аутентификация пользователей. Для каждого пользователя устанавливаются уникальные пароли. Они устанавливают принадлежность пользователя к информационной системе.

2. Разделение на группы пользователей. Пользователей делят на специальные группы. У каждой группы пользователей свой ограниченный функционал в системе. Это обеспечивает защиту информации. Каждый пользователь отвечает не за всю информацию в системе, а только за ту, с которой он непосредственно работает, и изменять он может только те документы и объекты конфигурации, с которыми он работает [20].

Кроме встроенных в систему методов защиты информации, на каждом компьютере пользователя установлено антивирусное программное обеспечение. Данное ПО обеспечивает защиту от угроз извне. Такие угрозы могут появиться при постоянной работе с интернетом и с внешними носителями.

Помимо программных средств защиты, на предприятии используются и физические средства защиты. На входе в каждый отдел в организации установлены электронные замки. Ключи от электронных замков в каждом отделе есть только у сотрудников данных отделов. Таким образом, исключается несанкционированный доступ к компьютеру каждого пользователя.

VI. ЗАКЛЮЧЕНИЕ

В статье были описаны требования к системе автоматизированного видеонализа нарушений техники безопасности, а также спроектирована архитектура решения. Главным выводом является тот факт, что процесс обеспечения и контроля безопасности на площадке строительства АЭС недостаточно автоматизирован и требует наличие информационной системы, с помощью которой может быть осуществлен процесс охраны труда с учетом особенностей предприятия. Предложенная авторами система предназначена для снижения количества случаев нарушения техники безопасности на строительных площадках, которые влекут за собой несчастные случаи и повышают степень травматизма.

Авторами было исследовано текущее состояние в организации с точки зрения автоматизации, проанализирована проблема и возможные решения, разработаны требования к функциям системы, описаны требования к инфраструктуре, разработан прототип решения.

Внедрение системы видеоналитики нарушений требований техники безопасности позволит повысить эффективность деятельности по обеспечению безопасности за счет снижения травматизма работников при производстве работ, а также за счет повышения трудовой дисциплины и культуры безопасности.

БИБЛИОГРАФИЯ

- [1] Калачева О. А. Охрана труда: причины производственного травматизма // Атуальные проблемы и перспективы развития транспорта, промышленности и экономики России ("ТрансПромЭк-2019"). – 2019. – С. 57-62.
- [2] Каримходжаев Н., Турахужаева Н. Н. Проблемы безопасности трудоемкости работников в предприятиях и некоторые пути их решения // *Universum: технические науки*. – 2020. – №. 4-1 (73). – С. 9-14.
- [3] Самарская Н. А., Ильин С. М. Формирование культуры охраны труда современных работников // *Новая наука: Теоретический и практический взгляд*. – 2017. – Т. 1. – №. 3. – С. 187-190.
- [4] Овсянникова О. В., Бычков А. В., Ефремова В. Н. Причины несчастных случаев на производстве // *Научно-методологические и социальные аспекты психологии и педагогики*. – 2017. – С. 53-56.
- [5] Яковлева Е. В., Быков М. О. Обзор примеров искусственного интеллекта управления безопасностью труда в АПК // *Вестник сельского развития и социальной политики*. – 2020. – №. 4 (28). – С. 26-28.
- [6] Тимофеев С. С., Тимофеева С. С. Цифровое будущее охраны труда // *XXI век. Техносферная безопасность*. – 2022. – Т. 7. – №. 1 (25). – С. 51-62.
- [7] Сазонова Е. А., Белобрыкин Н. Д. Обзор перспективных информационных технологий видеоаналитики // *Символ науки*. – 2021. – №. 3. – С. 37-40.
- [8] Забашта А. Ю., Скорикова С. А. Функции видеоаналитики, анализ архитектур систем видеоаналитики // *Ростовский научный журнал*. – 2017. – №. 7. – С. 194-200.
- [9] Габова О.С. Становление и перспективы развития центров (групп) автоматизированной фиксации административных правонарушений в области дорожного движения государственной инспекции безопасности дорожного движения // *Вестник Санкт-Петербургского университета МВД России*. 2017. №2 (74).
- [10] Hung C. C. et al. Videoedge: Processing camera streams using hierarchical clusters // *2018 IEEE/ACM Symposium on Edge Computing (SEC)*. – IEEE, 2018. – С. 115-131.
- [11] Видеоаналитика IDIS AI Вох для борьбы с COVID-19 // *IDIS Global*. 2021.
- [12] Рочев К. В. Информационные технологии. Анализ и проектирование информационных систем. – 2018.
- [13] Pavlov A. L. Recognition of Russian traffic signs in winter conditions. Solutions of the "Ice Vision" competition winners // *arXiv preprint arXiv:1909.07311*. – 2019.
- [14] Дорогов А. Ю., Харьковский А. С., Абатуров В. С. Аналитическая субд с сервис-ориентированной архитектурой // *Информационные технологии и информационная безопасность в науке, технике и образовании" ИНФОТЕХ-2017*". – 2017. – С. 10-14.
- [15] Шагилова Е. В. Принципы построения клиент/серверных систем // *Технологии XXI века: проблемы и перспективы развития*. – 2017. – С. 150-152.
- [16] Царев В., Веснин Е. Видеоаналитика – мощное оружие в борьбе с производственным травматизмом // *Control Engineering Россия*. – 2020. – №. 2. – С. 46-49.
- [17] Хлебников П. Увольнение за систематическое неисполнение указаний. Ошибки и споры // *Трудовое право*. – 2017. – №. 2. – С. 5.
- [18] Демиденко А. И., Кваша Е. П. Управление рисками информационной безопасности предприятий // *Российская наука: актуальные исследования и разработки*. – 2018. – С. 18-21.
- [19] Итальянцева В. С., Колмацуй А. И. Информационная безопасность как инструмент обеспечения экономической безопасности предприятия // *Актуальные вопросы права, экономики и управления*. – 2018. – С. 224-227.
- [20] Коджешау М. А. Технологии и алгоритмы информационной безопасности // *Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки*. – 2017. – №. 2 (201). – С. 129-135.

Development a video analytics system for violations of industrial safety requirements at nuclear power plant construction area

Anastasia Isakova, Vadim Sharmaev

Abstract — A construction area is an object of an increased risk zone for everyone who is on it, therefore, the security measures imposed on this territory must be strictly observed. Often, the process of observing safety precautions is formal and consists in conducting periodic briefings and training of personnel, and the function of direct control, as a rule, is assigned to immediate superiors. Video analytics and image processing technologies help to minimize these costs and increase the level of security by early warning of possible violations in the work of people or machines. Video analytics is a constantly evolving field where new methods and algorithms are constantly being developed in areas such as semantic video categorization, video retrieval from a database, human action recognition, generalization and anomaly detection. The article is devoted to the development of requirements for the system and architecture of the building control information system as part of the conceptual model. The authors investigated the current state of the organization in terms of automation, analyzed the problem and possible solutions, developed requirements for system functions, described infrastructure requirements, and developed a solution prototype. The introduction of a video analytics system for violations of safety requirements will improve the efficiency of safety activities by reducing employee injuries in the course of work, as well as by improving labor discipline and safety culture.

Keywords — video analytics system, safety precautions, system architecture, violation detection, incident analysis.

REFERENCES

- [1] Kalacheva O. A. Ohrana truda: prichiny proizvodstvennogo travmatizma // Aktual'nye problemy i perspektivy razvitiya transporta, promyshlennosti i jekonomiki Rossii ("TransPromJek-2019"). – 2019. – S. 57-62.
- [2] Karimhodzhaev N., Turahuzhaeva N. N. Problemy bezopasnosti trudodejatel'nosti rabotnikov v predpriyatijah i nekotorye puti ih reshenija // Universum: tehnicheckie nauki. – 2020. – #. 4-1 (73). – S. 9-14.
- [3] Samarskaja N. A., Il'in S. M. Formirovanie kul'tury ohrany truda sovremennyh rabotnikov // Novaja nauka: Teoreticheskij i prakticheskij vzgljad. – 2017. – T. 1. – #. 3. – S. 187-190.
- [4] Ovsjannikova O. V., Bychkov A. V., Efremova V. N. Prichiny neschastnyh sluchaev na proizvodstve // Nauchno-metodologicheskie i social'nye aspekty psihologii i pedagogiki. – 2017. – S. 53-56.
- [5] Jakovleva E. V., Bykov M. O. Obzor primerov iskusstvennogo intellekta upravlenija bezopasnost'ju truda v APK // Vestnik sel'skogo razvitiya i social'noj politiki. – 2020. – #. 4 (28). – S. 26-28.
- [6] Timofeev S. S., Timofeeva S. S. Cifrovoe budushhee ohrany truda // XXI vek. Tehnosfernaja bezopasnost'. – 2022. – T. 7. – #. 1 (25). – S. 51-62.
- [7] Sazonova E. A., Belobrykin N. D. Obzor perspektivnyh informacionnyh tehnologij videoanalitiki // Simvol nauki. – 2021. – #. 3. – S. 37-40.
- [8] Zabashta A. Ju., Skorikova S. A. Funkcii videoanalitiki, analiz arhitektur sistem videoanalitiki // Rostovskij nauchnyj zhurnal. – 2017. – #. 7. – S. 194-200.
- [9] Gabova O.S. Stanovlenie i perspektivy razvitiya centrov (grupp) avtomatizirovannoj fiksacii administrativnyh pravonarushenij v oblasti dorozhnogo dvizhenija gosudarstvennoj inspekcii bezopasnosti dorozhnogo dvizhenija // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2017. #2 (74).
- [10] Hung C. C. et al. Videoedge: Processing camera streams using hierarchical clusters // 2018 IEEE/ACM Symposium on Edge Computing (SEC). – IEEE, 2018. – S. 115-131.
- [11] Videoanalitika IDIS AI Box dlja bor'by s COVID-19 // IDIS Global. 2021.
- [12] Rochev K. V. Informacionnye tehnologii. Analiz i proektirovanie informacionnyh sistem. – 2018.
- [13] Pavlov A. L. Recognition of Russian traffic signs in winter conditions. Solutions of the "Ice Vision" competition winners // arXiv preprint arXiv:1909.07311. – 2019.
- [14] Dorogov A. Ju., Har'kovskij A. S., Abaturon V. S. Analiticheskaja subd s servis-orientirovannoj arhitekturoj // Informacionnye tehnologii i informacionnaja bezopasnost' v nauke, tehnike i obrazovanii" INFOTEH-2017". – 2017. – S. 10-14.
- [15] Shagilova E. V. Principy postroenija klient/servernyh sistem // Tehnologii XXI veka: problemy i perspektivy razvitiya. – 2017. – S. 150-152.
- [16] Carev V., Vesnin E. Videoanalitika – moshhnoe oruzhie v bor'be s proizvodstvennym travmatizmom //

Control Engineering Rossija. – 2020. – #. 2. – S. 46-49.

[17] Hlebnikov P. Uvol'nenie za sistematičeskoe neispolnenie ukazanij. Oshibki i spory // Trudovoe pravo. – 2017. – #. 2. – S. 5.

[18] Demidenko A. I., Kvasha E. P. Upravlenie riskami informacionnoj bezopasnosti predprijatij // Rossijskaja nauka: aktual'nye issledovanija i razrabotki. – 2018. – S. 18-21.

[19] Ital'janceva V. S., Kolmacuj A. I. Informacionnaja bezopasnost' kak instrument obespečenija jekonomičeskaj bezopasnosti predprijatija // Aktual'nye voprosy prava, jekonomiki i upravljenija. – 2018. – S. 224-227.

[20] Kodzheshau M. A. Tehnologii i algoritmy informacionnoj bezopasnosti // Vestnik Adygejskogo gosudarstvennogo universiteta. Serija 4: Estestvenno-matematičeskie i tehničeskie nauki. – 2017. – #. 2 (201). – S. 129-135.