УДК 004.8

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В КОНТРОЛЕ ОПАСНЫХ ЗОН И ПРЕДОТВРАЩЕНИИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Пачкин Е.Д. – студент гр. ПИб-232, III курс,
Научный руководитель: Глебова, Е.А., ст. преподаватель,
Кузбасский государственный технический университет имени Т.Ф. Горбачева
Россия, г. Кемерово

Вопрос контроля опасных зон на промышленном предприятии давно перестал быть чисто формальным требованием охраны труда. Реальные производственные площадки живут в режиме постоянных изменений: меняются технологические маршруты, оборудование переставляют, появляются временные рабочие места, на территорию заходят подрядные организации. На этом фоне классические средства безопасности – физические ограждения, таблички, периодические обходы – выполняют свою роль, но всё сложнее обеспечивают достаточный уровень контроля. Человек привыкает к обстановке, перестаёт замечать предупреждающие знаки, устаёт, отвлекается, а поток задач у службы безопасности только растёт [2-6].

Технологическое развитие подталкивает к более точному и одновременно гибкому подходу. Видеонаблюдение на большинстве предприятий уже есть, однако долгое время камеры работали лишь как «электронные глаза»: картинка писалась в архив, иногда просматривалась постфактум, когда что-то уже случилось. Переход к использованию нейросетевых технологий в корне меняет роль видеосистемы. Камера превращается в источник данных для анализа, а не просто в средство фиксации. Это позволяет сдвинуть акцент с расследования последствий на предупреждение инцидентов [2-4; 6].

Когда говорят об опасных зонах, обычно имеют в виду весьма конкретные пространства: рабочую зону станка, область перемещения стрелы крана, траекторию движения погрузчика, участок вокруг высокотемпературного агрегата. Вокруг таких мест формируются зоны, где нахождение человека без специальных допусков или средств индивидуальной защиты нежелательно или откровенно опасно. На практике именно в этих зонах и их «приграничных» областях происходят многие серьёзные случаи: работник заходит «буквально на минуту», проходит слишком близко к движущейся технике, задерживается в зоне, которая считалась только транзитной. Часть подобных ситуаций удаётся предотвратить за счёт дисциплины и инструктажей, но полностью исключить человеческий фактор невозможно [3-5; 9].

Нейросетевые методы компьютерного зрения дают возможность наблюдать за этими зонами непрерывно и без усталости. Алгоритмы детектируют на видеопотоке людей и технику, определяют их положение и соотносят его с заранее заданной картой опасных участков. Опасные зоны в такой системе

задаются не физическими ограждениями, а виртуальными контурами на изображении. Оператор однажды конфигурирует их в программном интерфейсе, при необходимости корректирует, а далее аналитика выполняется автоматически. Как только человек или транспортное средство пересекает виртуальную границу, система формирует событие: отображает предупреждение на экране, подаёт звуковой сигнал, отправляет уведомление ответственному сотруднику. При интеграции с оборудованием возможно и более жёсткое действие – например, остановка механизма при входе человека в область повышенного риска [2-4; 7; 8].

Важная особенность нейросетевых систем состоит в том, что они не ограничиваются разовой фиксированием факта «есть объект в зоне». Алгоритмы трекинга позволяют прослеживать траекторию движения человека или машины от кадра к кадру. Благодаря этому можно отличить случайное «касание» границы от осознанного входа в глубину опасной области, оценить скорость приближения к критическому месту, учесть направление движения. В ряде сценариев это критично: одно дело, когда работник пересёк край зоны и сразу вышел, и совсем другое – когда он идёт в сторону действующего крана или движущегося погрузчика. Система способна заранее «увидеть» сходящиеся траектории и среагировать ещё до того, как участники физически столкнутся [7-10].

Технически такая система складывается из нескольких слоёв. На нижнем уровне работают камеры, которые обеспечивают стабильное покрытие нужных участков. Где-то достаточно обычных IP-камер, а там, где условия сложнее – слабое освещение, пыль, дым – используются тепловизоры или комбинированные решения. Выше располагается вычислительная часть: либо локальные серверы на площадке, либо специализированные устройства рядом с камерами. Именно здесь выполняются нейросетевые модели, обрабатываются потоки данных и генерируются события. От выбранной архитектуры зависят задержка реакции и устойчивость к проблемам связи: при локальной обработке время от появления человека в зоне до тревоги может измеряться долями секунды [2; 3; 7].

Над аналитикой строится логика, понятная уже не инженеру, а специалисту по безопасности. В интерфейсе он видит схему площадки с выделенными опасными зонами, текущим положением объектов, журналом сработавших событий. Здесь же настраиваются правила: в какие часы какие зоны должны контролироваться, какие типы объектов считаются критичными, каким образом реагировать на каждую ситуацию. Для подрядчиков можно задать более жёсткие условия, для отдельных типов работ – временно разрешить пребывание в зоне при наличии наряда-допуска. Система фиксирует все случаи нарушения, что со временем формирует статистику и позволяет по-другому взглянуть на реальную картину безопасности на объекте [4-6].

Предотвращение несанкционированного доступа в опасную зону – это не только борьба с сознательными нарушителями. На практике значительная часть подобных эпизодов связана с невнимательностью, неточным представлением о границах ответственности или простым стремлением «срезать путь».

Камера с нейросетевой аналитикой не пытается угадать мотивы, но очень точно фиксирует факт появления человека там, где его не должно быть, и делает это вне зависимости от того, как именно он туда попал: через служебный проход, через приоткрытую секцию ограждения или через технологический проём. Первое предупреждение можно ограничить сигналом, при повторных нарушениях – формировать отчёты для руководства, использовать данные для дополнительного обучения персонала [2; 4; 9; 10].

Сами по себе нейросетевые технологии не являются волшебной «чёрной коробкой», которая без усилий решит все задачи безопасности. Их результат зависит от качества видеосигнала, правильного расположения камер, аккуратной настройки зон и грамотного выбора сценариев срабатывания. Любая модель ошибается; поэтому при внедрении неизбежно возникает вопрос баланса между пропущенными событиями и ложными тревогами. Слишком чувствительная система начнёт отвлекать персонал пустыми сигналами, слишком «толерантная» – не заметит часть реально опасных ситуаций. Этот баланс достигается через пилотную эксплуатацию, постепенную калибровку и регулярный пересмотр настроек по мере изменения производства [2; 3; 7; 8].

Есть и другие ограничения, которые нельзя игнорировать. Обработка видеопотоков в реальном времени требует существенных вычислительных ресурсов. Видеоаналитика с участием людей неизбежно затрагивает вопросы персональных данных и доступа к архивам. Интеграция системы в существующую инфраструктуру предприятия должна выполняться с учётом требований к кибербезопасности: вмешательство в работу механизмов останова или подмена видеосигнала теоретически могут привести не к повышению, а к снижению уровня безопасности. Всё это требует участия не только разработчиков и подрядчика по видеонаблюдению, но и службы ИТ, службы безопасности, охраны труда [4-6].

Несмотря на перечисленные сложности, накопленный опыт показывает, что при грамотном проектировании такие системы действительно меняют повседневную практику обеспечения безопасности. Появляется прозрачная картина фактического поведения людей и техники вблизи опасных зон, а не только формальное соответствие инструкциям. Руководитель участка может опираться не на единичные случаи и устные жалобы, а на статистику: где чаще всего происходят опасные пересечения, в какие смены нарушений больше, какие зоны требуют дополнительного физического ограждения, а где наоборот достаточно перенастройки маршрутов движения [2-5; 7-10].

Перспективы развития этого направления связаны с дальнейшим объединением видеоаналитики с другими источниками информации. Данные о попадании в опасную зону можно сопоставлять с показаниями датчиков оборудования, системой контроля доступа, графиками технологических операций. На этом уровне уже речь идёт не только о фиксации нарушений, но и о построении моделей риска: какие сочетания факторов чаще всего приводят к инцидентам, какие сценарии следует предотвращать в первую очередь. По мере того как цифровые двойники производственных участков становятся практическим

инструментом, данные нейросетевой аналитики могут стать одним из ключевых слоёв, описывающих реальное поведение людей и техники в этом цифровом представлении [7-10].

В итоге нейросетевые технологии в контроле опасных зон и предотвращении несанкционированного доступа не заменяют классические средства безопасности, а дополняют их, закрывая те области, где человеческий контроль неизбежно ослабевает. При аккуратном внедрении, с учётом технических, организационных и правовых аспектов, такие системы превращаются из очередной в рабочий инструмент, который помогает объективно видеть риски и действительно снижать вероятность тяжёлых происшествий на производстве [2-6; 9; 10].

Список литературы:

1. Гудфеллоу Я., Бенджио И., Курвилл А. Глубокое обучение / Пер. с англ. – М.: ДМК Пресс, 2018. – 652 с. – ISBN 978-5-97060-554-1.

2. Вульфин А.М. Интеллектуальный анализ видеоданных в системе контроля соблюдения правил промышленной безопасности // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8, № 2 (29). – С. 1–16.

3. Исакова А.Ю., Шармаев В.И. Проектирование системы видеоаналитики нарушений требований промышленной безопасности на площадках сооружения АЭС // International Journal of Open Information Technologies. – 2022. – № 8. – С. 77–83.

4. Юрьев С.С., Газя Г.В. Внедрение системы видеоаналитики для контроля доступа в зоны промышленной опасности // Вестник науки. – 2025. – № 6 (87). – Т. 4. – С. 2015–2020. – Текст: электронный. – URL: https://www.вестник-науки.рф/article/24787 (дата обращения: 13.11.2025).

5. Видеоаналитика в горнодобывающей промышленности: безопасность, эффективность и автоматизация / Редакция журнала «Золотодобыча» // Золотодобыча. – 2025. – № 6 (319). – Текст: электронный. – URL: https://xn–80abilurbab1b9c5b.xn–p1acf/index.php/supply-construction-implementation/video-analytics-in-the-mining-industry-safety-efficiency-and-automation-menu (дата обращения: 14.11.2025).

6. Демидова А., Волкинд Я., Юдин А. Нейросетевые технологии проникают и в сферу охраны труда // Secuteck.ru. – 2024. – 14 нояб. – Текст: электронный. – URL: https://www.secuteck.ru/articles/nejrosetevye-tekhnologii-pronikayut-i-v-sferu-ohrany-truda (дата обращения: 15.11.2025).

7. Abbas M.S., Hussain R., Zaidi S.F.A., Lee D., Park C. Computer Vision-Based Safety Monitoring of Mobile Scaffolding Integrating Depth Sensors // Buildings. – 2025. – Vol. 15, No. 13. – Art. 2147. – DOI: 10.3390/buildings15132147.

8. Lee J. Construction Site Safety Management: A Computer Vision and Deep Learning Approach // Sensors. – 2023. – Vol. 23, No. 2. – Art. 944. – DOI: 10.3390/s23020944.

9. Vukicevic A.M., Petrovic M., Milosevic P., Peulic A., Jovanovic K., Novakovic A. A Systematic Review of Computer Vision-Based Personal Protective Equipment Compliance in Industry Practice: Advancements, Challenges and Future Directions // Artificial Intelligence Review. – 2024. – Vol. 57. – Art. 319. – DOI: 10.1007/s10462-024-10978-x