УДК 004.8:37.06
МРНТИ 14.35.07
DOI 10.56525/OPLJ5486

ИСПОЛЬЗОВАНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ГРАЖДАН НА ОСНОВЕ АНАЛИЗА ВИДЕОПОТОКОВ

Дусекенова Э.П.
Казахстанский университет инновационных и телекоммуникационных систем, Орал, Казакстан
e-mail: elvira.dusekenova.03@bk.ru

Аннотация. В современных условиях стремительного роста урбанизации и увеличения плотности населения проблема обеспечения безопасности граждан в общественных местах приобретает особую актуальность. Традиционные системы видеонаблюдения, основанные на участии человека-оператора, зачастую не позволяют своевременно и эффективно обрабатывать большие объемы видеоданных, что снижает вероятность оперативного реагирования на потенциальные угрозы. В этой связи особый интерес представляет использование систем искусственного интеллекта, способных автоматически анализировать видеопотоки в режиме реального времени.

В статье рассматриваются подходы к применению методов компьютерного зрения и машинного обучения для повышения уровня общественной безопасности. Особое внимание уделяется технологиям детекции и классификации объектов, а также распознаванию действий и поведенческих паттернов, таких как агрессивное поведение, драки, подозрительная активность и другие потенциально опасные ситуации. Описываются принципы построения интеллектуальных систем, включающих этапы сбора и подготовки данных, обучения моделей и их внедрения в реальные условия эксплуатации.

Также анализируются преимущества использования подобных решений, включая снижение нагрузки на операторов, повышение точности выявления инцидентов и возможность масштабирования системы на большое количество камер. Отдельно рассматриваются вопросы надежности, минимизации ложных срабатываний и адаптации моделей к различным условиям видеосъемки, таким как освещение, угол обзора и качество изображения.

Результаты исследования показывают, что внедрение систем искусственного интеллекта в сферу видеонаблюдения способствует значительному повышению эффективности мониторинга общественных пространств и позволяет обеспечить более быстрый отклик на возникающие угрозы. В заключении подчеркивается потенциал дальнейшего развития данных технологий и их роль в формировании безопасной городской среды.

Ключевые слова: искусственный интеллект, компьютерное зрение, анализ видеопотоков, видеонаблюдение, безопасность граждан, распознавание действий, интеллектуальные системы.

Введение

В условиях стремительного развития цифровых технологий и роста урбанизации обеспечение безопасности граждан становится одной из ключевых задач современного общества. Особенно актуальной данная проблема является в общественных пространствах, включая образовательные учреждения, где ежедневно взаимодействует большое количество людей. Несмотря на существование традиционных мер контроля, таких как видеонаблюдение и физическое присутствие персонала, уровень угроз, включая агрессивное поведение, правонарушения и буллинг, остаётся значительным [1]. При этом существующие системы

видеонаблюдения, как правило, требуют постоянного участия человека-оператора, что делает процесс анализа видеоданных неэффективным в условиях большого потока информации [2]. Ограниченность человеческого внимания, усталость и высокая нагрузка приводят к тому, что многие инциденты остаются незамеченными или фиксируются с опозданием, что снижает общий уровень безопасности.

В последние годы особую актуальность приобрела проблема буллинга и агрессивного поведения, особенно в образовательной среде. Буллинг представляет собой систематическое проявление агрессии, включающее психологическое давление, оскорбления, насмешки, а также физическое насилие [3]. Исследования показывают, что значительная часть учащихся хотя бы один раз сталкивается с подобными ситуациями в процессе обучения [4]. При этом наиболее распространённой формой является психологический буллинг, в то время как физическое насилие и кибербуллинг также занимают значительную долю. Соотношение различных форм буллинга может быть наглядно представлено (график). Следует отметить, что многие случаи агрессии остаются скрытыми, поскольку учащиеся не всегда сообщают о происходящем, а педагоги не имеют возможности контролировать все зоны учебного заведения [5].

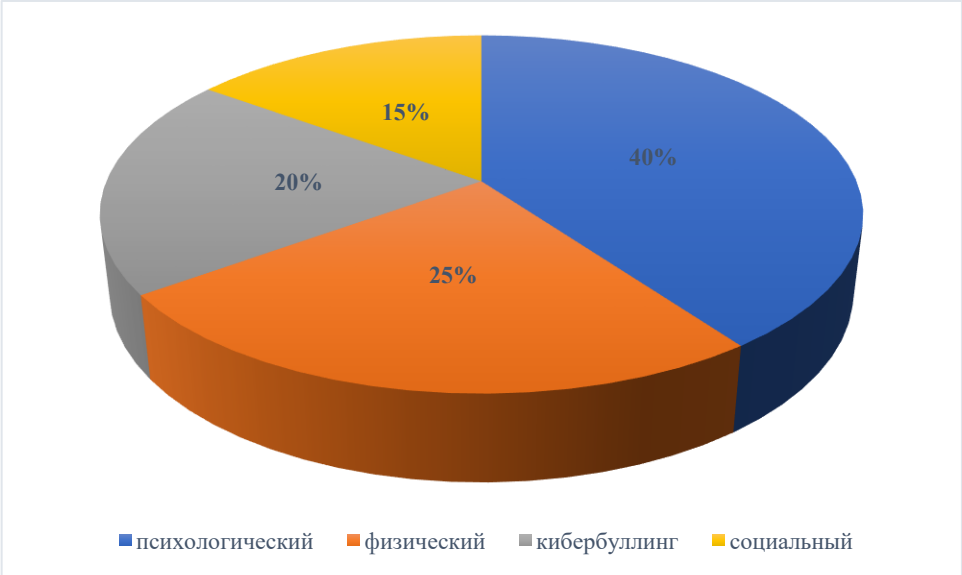

Рисунок 1. Распределение форм буллинга среди школьников (по условным данным опросов)

Традиционные методы профилактики, включающие воспитательные беседы, участие школьных психологов и образовательные программы, играют важную роль, однако их эффективность часто оказывается недостаточной [6]. Это связано с тем, что значительная часть конфликтов происходит вне зоны непосредственного контроля взрослых. В последние годы наблюдается рост числа подобных инцидентов, что подтверждается статистическими данными (график), и свидетельствует о необходимости внедрения новых технологических решений [7]. В условиях цифровизации образования особое значение приобретает использование интеллектуальных систем, способных автоматически анализировать происходящее в режиме реального времени.

Развитие технологий искусственного интеллекта открывает новые возможности для повышения эффективности систем видеонаблюдения. Методы компьютерного зрения позволяют анализировать видеопотоки, распознавать объекты, отслеживать движение и выявлять поведенческие паттерны [8]. Одним из наиболее эффективных подходов является использование нейронных сетей глубокого обучения, способных обрабатывать визуальные данные с высокой точностью [9]. Современные модели детекции объектов, такие как YOLO, позволяют в реальном времени обнаруживать людей, предметы и потенциально опасные

объекты [10]. Одновременно с этим модели распознавания действий анализируют последовательность кадров и позволяют определить характер происходящего, включая агрессивные действия, толчки и драки [11].

Принцип работы интеллектуальной системы анализа видеопотоков заключается в последовательной обработке видеоданных, включающей извлечение кадров, их анализ с помощью нейронных сетей, классификацию ситуации и формирование сигнала тревоги при обнаружении потенциальной угрозы. Данный процесс может быть представлен в обобщённом виде.

Таблица 1 – Преимущества и риски использования ИИ в школах

Преимущества	**Возможные риски и вызовы**
Своевременное выявление агрессии	Нарушение конфиденциальности
Повышение безопасности учащихся	Ошибки алгоритмов и ложные срабатывания
Снижение нагрузки на педагогов	Правовые пробелы в регулировании
Формирование культуры ненасилия	Этические вопросы приватности

Использование таких систем позволяет значительно повысить эффективность мониторинга и сократить время реакции на инциденты.

Важным направлением развития систем анализа видеопотоков является повышение интерпретируемости результатов работы искусственного интеллекта. В условиях практического применения недостаточно только факта обнаружения потенциально опасной ситуации, необходимо также понимать, по каким признакам система приняла то или иное решение. Это особенно актуально в случаях, когда речь идёт о спорных ситуациях или возможных ошибках алгоритма. Современные подходы к объяснимому искусственному интеллекту позволяют визуализировать области кадра, на которые модель обращает наибольшее внимание, а также анализировать вклад отдельных признаков в итоговое решение. Подобные механизмы повышают доверие к системе и упрощают процесс её внедрения в реальные условия.

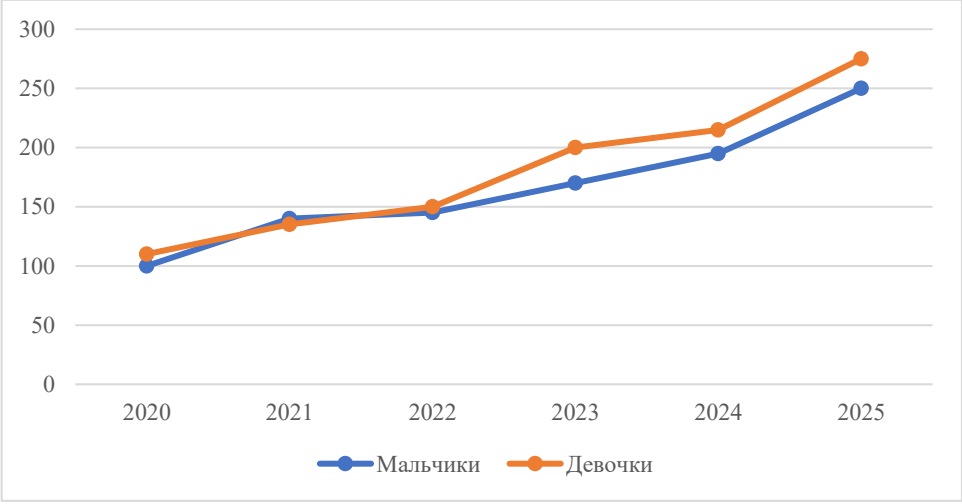

Рисунок 2. Динамика кибербуллинга в Казахстане за 2020 – 2025 годы

Отдельное внимание следует уделить вопросам оценки эффективности работы интеллектуальных систем. Для этого используются различные метрики качества, отражающие точность и надёжность распознавания. В контексте задач обнаружения агрессии и опасных ситуаций особую значимость приобретают показатели полноты и точности, позволяющие оценить баланс между пропущенными инцидентами и ложными срабатываниями. Анализ

зависимости этих показателей может быть представлен (график), что позволяет выбрать оптимальные параметры работы системы в зависимости от требований конкретного объекта.

Существенным аспектом является также временная устойчивость моделей. Видеопоток представляет собой последовательность кадров, и корректная интерпретация происходящего требует учёта динамики изменений. В связи с этим применяются методы, позволяющие анализировать не отдельные изображения, а их последовательности, что даёт возможность выявлять закономерности движения и изменения поведения. Такой подход позволяет более точно различать случайные действия и целенаправленную агрессию, снижая вероятность ошибочной классификации.

Важным направлением является адаптация систем к различным социальным и культурным контекстам. Поведение людей может существенно различаться в зависимости от среды, возраста и особенностей взаимодействия, что необходимо учитывать при обучении моделей. Универсальные алгоритмы не всегда способны корректно интерпретировать такие различия, поэтому требуется их дополнительная настройка и адаптация. Это особенно актуально для образовательных учреждений, где поведенческие нормы отличаются от других общественных пространств.

В процессе эксплуатации систем возникает необходимость их постоянного обновления и доработки. Это связано с тем, что модели могут терять актуальность при изменении условий или появлении новых типов поведения. Для решения данной проблемы используются методы непрерывного обучения, позволяющие постепенно улучшать качество работы системы на основе новых данных. Такой подход обеспечивает её долгосрочную эффективность и адаптивность.

Отдельно следует рассмотреть вопросы хранения и обработки видеоданных. Большие объёмы информации требуют использования специализированных решений, обеспечивающих надёжность и безопасность хранения. При этом важно учитывать не только технические, но и правовые аспекты, связанные с ограничением сроков хранения данных и контролем доступа к ним.

Также значительное внимание уделяется вопросам кибербезопасности. Системы, обрабатывающие видеоданные, могут являться объектом атак, направленных на получение доступа к конфиденциальной информации или нарушение их работы. В связи с этим необходимо внедрение механизмов защиты, включая шифрование данных, аутентификацию пользователей и контроль целостности информации. Надёжность системы напрямую влияет на уровень доверия к ней и возможность её широкого применения.

Не менее важным является аспект взаимодействия системы с пользователями. Интерфейс должен быть интуитивно понятным и обеспечивать удобный доступ к информации. Важной функцией является возможность фильтрации событий, поиска по временным интервалам и формирования аналитических отчётов. Это позволяет не только оперативно реагировать на инциденты, но и проводить последующий анализ для выявления закономерностей и принятия управленческих решений.

Следует также отметить роль искусственного интеллекта в прогнозировании потенциально опасных ситуаций. На основе анализа накопленных данных система может выявлять закономерности, предшествующие конфликтам, и сигнализировать о повышенном уровне риска. Такой подход позволяет перейти от реактивной модели безопасности к проактивной, что значительно повышает её эффективность.

Дополнительным направлением является интеграция систем видеонаблюдения с другими цифровыми сервисами. Это может включать взаимодействие с системами контроля доступа, оповещения и управления безопасностью. Комплексный подход позволяет создать единую экосистему, обеспечивающую высокий уровень защиты и оперативного реагирования.

Одним из ключевых преимуществ применения искусственного интеллекта является возможность работы в режиме реального времени, что обеспечивает оперативное выявление опасных ситуаций [12]. В отличие от человека, алгоритмы способны анализировать большие объёмы данных без снижения точности и не подвержены усталости. Кроме того, системы ИИ

позволяют выявлять ранние признаки агрессии, что даёт возможность предотвратить развитие конфликта до его эскалации [13]. Это особенно важно в образовательной среде, где своевременное вмешательство может существенно снизить уровень насилия и улучшить психологический климат.

Дополнительным преимуществом является возможность масштабирования подобных решений. Интеллектуальные системы могут быть интегрированы в существующую инфраструктуру видеонаблюдения и использоваться одновременно на большом количестве камер. Эффективность применения таких технологий может быть наглядно продемонстрирована на основе сравнительных данных (график), отражающих снижение числа инцидентов после внедрения ИИ-систем [14].

Несмотря на значительные преимущества, использование искусственного интеллекта в системах видеонаблюдения связано с рядом проблем. Одной из основных является наличие ложных срабатываний, когда система ошибочно классифицирует безопасную ситуацию как опасную [15]. Это может привести к снижению доверия к системе и увеличению нагрузки на персонал. Также следует учитывать зависимость качества работы алгоритмов от условий видеосъёмки, включая освещение, угол обзора и качество изображения [16]. Низкое качество данных может существенно снизить точность распознавания и привести к ошибкам.

Кроме того, для обучения моделей требуется большое количество размеченных данных, что делает процесс разработки сложным и ресурсоёмким [17]. Важной задачей является также адаптация моделей к различным условиям эксплуатации и типам видеопотоков.

Особое внимание необходимо уделять правовым и этическим аспектам использования подобных технологий. В Республике Казахстан действует закон «О персональных данных и их защите», который регулирует вопросы сбора, хранения и обработки информации [18]. Использование систем видеонаблюдения с элементами искусственного интеллекта должно соответствовать требованиям конфиденциальности и обеспечивать защиту частной жизни граждан. В образовательной среде особое значение имеет получение согласия родителей на обработку данных учащихся [19].

Этические аспекты связаны с необходимостью соблюдения баланса между обеспечением безопасности и правом на личное пространство. Важно обеспечить прозрачность работы системы и исключить возможность её неправомерного использования [20]. Также необходимо учитывать риски, связанные с автоматизированным принятием решений и возможными ошибками алгоритмов.

В условиях активной цифровизации образования в Казахстане существует значительный потенциал для внедрения интеллектуальных систем безопасности. Перспективным направлением является создание комплексных платформ, объединяющих видеонаблюдение, аналитику на основе искусственного интеллекта, психологическую поддержку и систему реагирования [21]. Такой подход позволит не только снизить уровень агрессии, но и сформировать безопасную образовательную среду.

Развитие технологий искусственного интеллекта в ближайшие годы приведёт к повышению точности моделей, снижению количества ложных срабатываний и расширению функциональных возможностей систем [22]. Ожидается интеграция различных источников данных, включая аудио и сенсорные устройства, что позволит более полно анализировать происходящее [23]. Важным направлением также является разработка методов объяснимого искусственного интеллекта, позволяющих интерпретировать решения системы [24].

Применение искусственного интеллекта в школьных системах видеонаблюдения создаёт новые возможности для предотвращения буллинга и проявления агрессии [8–10; 23]. Внедрение таких технологий позволяет усилить меры безопасности, обеспечивать психологическое благополучие учащихся и формировать более благоприятный и безопасный образовательный климат. Наряду с этим важно учитывать правовые нормы и строго следовать этическим стандартам при их применении [22; 24; 25]. В связи с этим проблема выявления социальных конфликтов в подростковой среде является важным направлением профилактики

агрессивного поведения, поскольку своевременное обнаружение конфликтных ситуаций позволяет снизить риск их дальнейшей эскалации [26]. Эффективная реализация подобных инициатив в образовательных учреждениях Казахстана возможна лишь при комплексном подходе, сочетающем современные технические решения с продуманными социально-правовыми механизмами.

ЛИТЕРАТУРА

1. Овчарова Р.В. Психология буллинга: причины, последствия и профилактика. – М.: Академический проект, 2020. – 256 с.

2. Кулагина И.Ю., Колюцкий В.Н. Психология развития и возрастная психология. – М.: Юрайт, 2019. – 447 с.

3. Карабанова О.А. Психология семейных отношений и основы семейного консультирования. – М.: Гардарики, 2018. – 320 с.

4. Сластенин В.А., Исаев И.Ф., Шиянов Е.Н. Педагогика. – М.: Академия, 2017. – 576 с.

5. Фельдштейн Д.И. Психология развития человека. – М.: Институт практической психологии, 2016. – 512 с.

6. Полат Е.С. Современные педагогические и информационные технологии в системе образования. – М.: Академия, 2020. – 368 с.

7. Беспалько В.П. Слагаемые педагогической технологии. – М.: Педагогика, 2018. – 192 с.

8. Гаврилов А.В. Компьютерное зрение и обработка изображений. – М.: ДМК Пресс, 2021. – 384 с.

9. Васильев В.Н., Сафонов И.В. Интеллектуальные системы видеонаблюдения. – СПб.: БХВ-Петербург, 2020. – 312 с.

10. Иванов В.В. Методы машинного обучения в задачах анализа данных. – М.: Физматлит, 2019. – 256 с.

11. Петров А.А. Искусственный интеллект: современные методы и технологии. – М.: Наука, 2021. – 420 с.

12. Капустин А.В. Системы безопасности и видеонаблюдения. – М.: Инфра-М, 2018. – 280 с.

13. Берди Д., Есимова А., Турсынова А. Цифровая гигиена и снижение кибербуллинга среди подростков // Международный журнал оценки и исследований в образовании. – 2023. – Т. 12, №3. – С. 1010–1017.

14. Кумысбеков Т., Сабитов З., Акимжанова Г. Проблемы профилактики кибербуллинга на современном этапе // Вестник Карагандинского университета. Серия «Право». – 2022. – №1(105). – С. 55–62.

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

16. Хиндуджа С., Патчин Дж. Буллинг за пределами школы: предотвращение и реагирование на кибербуллинг. – Thousand Oaks: Corwin Press, 2014. – 304 с.

17. Лахби М., Патан А.-С.К., Малех Ю. Противодействие кибербуллингу в цифровых медиа с использованием искусственного интеллекта. – Boca Raton: CRC Press, 2024. – 356 с.

18. Уайсса М. Борьба с кибербуллингом с использованием генеративного искусственного интеллекта. – Hershey: IGI Global, 2025. – 298 с.

19. Дас Р. Генеративный искусственный интеллект и кибербуллинг. – London: Routledge, 2024. – 214 с.

20. Наварро Р. Семья, буллинг и кибербуллинг. – Basel: MDPI, 2019. – 232 с.

21. Гудфеллоу И., Бенджио Й., Курвилль А. Глубокое обучение. – Cambridge: MIT Press, 2016. – 800 с.

22. Сзелиски Р. Компьютерное зрение: алгоритмы и приложения. – Cham: Springer, 2022. – 979 с.

23. Редмон Дж., Дивалла С., Гиршик Р., Фархади А. You Only Look Once: единый метод детекции объектов в реальном времени // Труды IEEE CVPR. – 2016. – С. 779–788.

24. Рассел С., Норвиг П. Искусственный интеллект: современный подход. – Hoboken: Pearson, 2021. – 1152 с.

25. ЮНЕСКО. Искусственный интеллект в образовании: руководство для разработчиков политики. – Париж: UNESCO, 2021. – 120 с.

26. Кокшеева З.Т., Демиханова А.У. Выявление социальных конфликтов и путей их разрешения в подростковой среде // Yessenov Science Journal №2 (51). – 2025. – С. 167–174.

REFERENCES

1. Ovcharova R.V. Psikhologiya bullinga: prichiny, posledstviya i profilaktika. – Moscow: Akademicheskiy proekt, 2020. – 256 p.

2. Kulagina I.Yu., Kolyutskiy V.N. Psikhologiya razvitiya i vozrastnaya psikhologiya. – Moscow: Yurayt, 2019. – 447 p.

3. Karabanova O.A. Psikhologiya semeynykh otnosheniy i osnovy semeynogo konsultirovaniya. – Moscow: Gardariki, 2018. – 320 p.

4. Slastenin V.A., Isaev I.F., Shiyanov E.N. Pedagogika. – Moscow: Akademiya, 2017. – 576 p.

5. Feldshteyn D.I. Psikhologiya razvitiya cheloveka. – Moscow: Institut prakticheskoy psikhologii, 2016. – 512 p.

6. Polat E.S. Sovremennye pedagogicheskie i informatsionnye tekhnologii v sisteme obrazovaniya. – Moscow: Akademiya, 2020. – 368 p.

7. Bespalko V.P. Slagaemye pedagogicheskoy tekhnologii. – Moscow: Pedagogika, 2018. – 192 p.

8. Gavrilov A.V. Kompyuternoe zrenie i obrabotka izobrazheniy. – Moscow: DMK Press, 2021. – 384 p.

9. Vasiliev V.N., Safonov I.V. Intellektualnye sistemy videonablyudeniya. – Saint Petersburg: BHV-Peterburg, 2020. – 312 p.

10. Ivanov V.V. Metody mashinnogo obucheniya v zadachakh analiza dannykh. – Moscow: Fizmatlit, 2019. – 256 p.

11. Petrov A.A. Iskusstvennyy intellekt: sovremennye metody i tekhnologii. – Moscow: Nauka, 2021. – 420 p.

12. Kapustin A.V. Sistemy bezopasnosti i videonablyudeniya. – Moscow: Infra-M, 2018. – 280 p.

13. Berdi D., Yesimova A., Tursynova A. Tsifrovaya gigiena i snizhenie kiberbullinga sredi podrostkov // International Journal of Evaluation and Research in Education. – 2023. – Vol. 12, No. 3. – P. 1010–1017.

14. Kumysbekov T., Sabitov Z., Akimzhanova G. Problemy profilaktiki kiberbullinga na sovremennom etape // Vestnik Karagandinskogo universiteta. Seriya «Pravo». – 2022. – No. 1(105). – P. 55–62.

15. Zakon Respubliki Kazakhstan «O personalnykh dannykh i ikh zashchite» ot 21 maya 2013 goda No. 94-V.

16. Khindudzha S., Patchin J. Bulling za predelami shkoly. – Thousand Oaks: Corwin Press, 2014. – 304 p.

17. Lakhbi M., Patan A.-S.K., Maleh Yu. Protivodeystvie kiberbullingu v tsifrovykh media. – Boca Raton: CRC Press, 2024. – 356 p.

18. Uaissa M. Borba s kiberbullingom s ispolzovaniem generativnogo II. – Hershey: IGI Global, 2025. – 298 p.

19. Das R. Generativnyy iskusstvennyy intellekt i kiberbulling. – London: Routledge, 2024. – 214 p.

20. Navarro R. Semya, bulling i kiberbulling. – Basel: MDPI, 2019. – 232 p.

21. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge: MIT Press, 2016. – 800 p.

22. Szeliski R. Computer Vision: Algorithms and Applications. – Cham: Springer, 2022. – 979 p.

23. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once // IEEE CVPR. – 2016. – P. 779–788.

24. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – Hoboken: Pearson, 2021. – 1152 p.

25. UNESCO. Artificial Intelligence in Education. – Paris: UNESCO, 2021. – 120 p.

26. Koksheyeva Z.T., Demikhanova A.U. Identification of Social Conflicts and Ways of Their Resolution in the Adolescent Environment // Yessenov Science Journal No. 2 (51). – 2025. – pp. 167–174.

БЕЙНЕАҒЫНДАРДЫ ТАЛДАУ НЕГІЗІНДЕ АЗАМАТТАРДЫҢ ҚАУІПСІЗДІГІН АРТТЫРУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТ ЖҮЙЕЛЕРІН ПАЙДАЛАНУ

Дусекенова Э.П.
"Қазақстан инновациялық және телекоммуникациялық жүйелер университеті,
Орал, Қазақстан
e-mail: elvira.dusekenova.03@bk.ru

Аннотация. Қазіргі таңда урбанизацияның қарқынды дамуы және халық тығыздығының артуы жағдайында қоғамдық орындардағы азаматтардың қауіпсіздігін қамтамасыз ету аса өзекті мәселелердің біріне айналып отыр. Дәстүрлі бейнебақылау жүйелері, негізінен, адам-операторлардың қатысуына сүйенетіндіктен, үлкен көлемдегі бейнемәліметтерді уақтылы және тиімді өңдеуге әрдайым мүмкіндік бермейді. Бұл өз кезегінде ықтимал қауіптерге жедел әрекет ету мүмкіндігін төмендетеді. Осыған байланысты бейнеағындарды нақты уақыт режимінде автоматты түрде талдай алатын жасанды интеллект жүйелерін қолдану ерекше маңызға ие.

Мақалада қоғамдық қауіпсіздікті арттыру мақсатында компьютерлік көру және машиналық оқыту әдістерін қолдану тәсілдері қарастырылады. Агрессивті мінез-құлық, төбелес, күмәнді әрекеттер сияқты қауіпті жағдайларды анықтауға арналған объектілерді детекциялау, жіктеу және әрекеттерді тану технологияларына ерекше назар аударылады. Сонымен қатар, интеллектуалды жүйелерді құрудың негізгі кезеңдері, атап айтқанда деректерді жинау және дайындау, модельдерді оқыту және оларды нақты жағдайларда қолдану ерекшеліктері сипатталады.

Сондай-ақ мұндай жүйелерді қолданудың артықшылықтары талданады, олардың қатарына операторларға түсетін жүктемені азайту, инциденттерді анықтау дәлдігін арттыру және жүйені көптеген бейнекамераларға бейімдеу мүмкіндігі жатады. Бөлек түрде жалған анықтауларды азайту, жүйенің сенімділігін арттыру және әртүрлі бейнежазба шарттарына (жарықтандыру, түсіру бұрышы, кескін сапасы) бейімделу мәселелері қарастырылады.

Зерттеу нәтижелері жасанды интеллект негізіндегі бейнебақылау жүйелерін енгізу қоғамдық кеңістіктерді бақылаудың тиімділігін едәуір арттыратынын және қауіптерге жедел әрекет етуге мүмкіндік беретінін көрсетеді. Қорытынды бөлімде аталған технологиялардың

әрі қарай даму әлеуеті және олардың қауіпсіз қалалық ортаны қалыптастырудағы рөлі атап өтіледі.

Түйін сөздер: жасанды интеллект, компьютерлік көру, бейнеағындарды талдау, бейнебақылау, азаматтардың қауіпсіздігі, әрекеттерді тану, интеллектуалды жүйелер.

USING ARTIFICIAL INTELLIGENCE SYSTEMS TO ENHANCE PUBLIC SAFETY BASED ON VIDEO STREAM ANALYSIS

Dussekenova E.P.
"Kazakhstan University of Innovative and Telecommunication Systems, Oral, Kazakhstan
e-mail: elvira.dusekenova.03@bk.ru

Annotation. In the context of rapid urbanization and increasing population density, ensuring public safety in urban environments has become a critically important task. Traditional video surveillance systems, which rely heavily on human operators, are often unable to efficiently process large volumes of video data in real time, reducing the effectiveness of timely threat detection and response. In this regard, the use of artificial intelligence systems capable of automatically analyzing video streams offers significant potential for improving public safety.

This paper explores approaches to applying computer vision and machine learning techniques to enhance the effectiveness of surveillance systems. Particular attention is given to technologies for object detection and classification, as well as action and behavior recognition, including the identification of aggressive behavior, physical altercations, and other potentially dangerous activities. The study also outlines the key stages involved in developing intelligent video analysis systems, including data collection and preprocessing, model training, and deployment in real-world environments.

In addition, the advantages of such systems are analyzed, including reduced workload for human operators, improved accuracy in incident detection, and scalability across large camera networks. Special consideration is given to challenges such as minimizing false positives, ensuring system reliability, and adapting models to varying video conditions, including lighting, camera angles, and image quality.

The results demonstrate that integrating artificial intelligence into video surveillance systems significantly enhances monitoring efficiency and enables faster response to emerging threats. The paper concludes by highlighting the future development potential of these technologies and their important role in creating safer urban environments.

Key words: artificial intelligence, computer vision, video stream analysis, video surveillance, public safety, action recognition, intelligent systems.