МРНТИ 50.41.17

**А.Б. Рустемов*, Б.А. Кузенбаев**

*Костанайский региональный университет имени А. Байтурсынова, Костанай, Казахстан*
*E-mail: *rustemov_azat@mail.ru, bekz@bk.ru*

# Принципы определения подозрительной активности и программы для анализа подозрительной активности с помощью камер видеонаблюдения

**Аннотация**. *В предложенной статье обсуждаются принципы определения подозрительной активности с точки зрения логики и психологии человека, а также исследуются существующие программы для анализа подозрительной активности с помощью камер видеонаблюдения. Рассматриваются основные виды подозрительной активности, такие, как скопление людей, быстрое передвижение, проникновение на охраняемую территорию и оставленные без присмотра вещи, а также методы и инструменты, которые можно использовать для их обнаружения. В исследовании затрагиваются преимущества и недостатки существующих популярных программ анализа подозрительной активности посредством видеонаблюдения, в том числе обсуждается концепция программы, которая могла бы конкурировать с другими программами в этом направлении, привнося новшества, используя преимущества конкурентов и не допуская недостатки соперников.*

**Ключевые слова:** *подозрительная активность, камеры видеонаблюдения, анализ поведения людей, безопасность, машинное обучение.*

**DOI: doi.org/10.32523/2616-7263-2023-144-3-100-110**

## 1. Введение

Современные камеры видеонаблюдения являются незаменимым инструментом для обеспечения безопасности на объектах различного назначения: от банков и магазинов до государственных учреждений и жилых домов. Однако многие системы видеонаблюдения просто записывают видеопоток, не предоставляя информацию о подозрительных событиях. Для того, чтобы детектировать и реагировать на потенциально опасные события, требуются специализированные программы, которые могут обрабатывать видеопоток и автоматически определять подозрительную активность.

Для написания таких программ нужно знать принципы, по которым можно классифицировать человека как подозрительного, а в дальнейшем возможно и потенциально опасного.

В данной статье будут рассмотрены принципы определения подозрительной активности с точки зрения логики и человеческой психологии. Также будет исследование уже существующих решений для анализа подозрительной активности человека с помощью видеонаблюдения. В результате этого будет сформирована концепция модели программы, которая могла бы конкурировать с другими программами в этом направлении, привнося новшества, используя преимущества конкурентов и не допуская недостатки соперников.

## 2. Методы

Определение подозрительной активности может быть субъективным, так как каждый человек имеет свою точку зрения на окружающий мир. Согласно толковому словарю русского языка Дмитриева Д.В., подозрительным могут считаться любые действия, проявляющие недоверие или сомнения в отношении чего-то или кого-то. В зависимости от жизненного опыта и знаний человека, любая активность может быть названа подозрительной [1].

Однако в профессиях, где любая ошибка может привести к серьезным последствиям, необходимо обучать специалистов определять подозрительное поведение. Например, в аэропортах по всему миру используют систему SPOT [2], которая содержит 94 критерия подозрительного поведения, таких, как частое моргание, зевание, свист, нервный тик и другие. Это позволяет сотрудникам аэропортов задавать вопросы и проверять багаж подозрительных пассажиров, что существенно снижает количество происшествий. Таким образом, важно обучать специалистов профессионально общаться с людьми и определять подозрительное поведение, чтобы минимизировать возможность ошибок, особенно в ответственных сферах, таких, как полиция, медицина, военные и охранные службы.

Многие разработчики систем безопасности по-прежнему задаются вопросом о том, как научить машину определять подозрительное поведение. Однако уже существуют логические методы, которые успешно используются для обнаружения подозрительной активности. Изучив подозрительную активность с точки зрения логики и психологии, можно найти несколько методов определения подозрительной активности, которые будут включать в себя:

- мониторинг скопления людей;
- учет количества входящих и выходящих людей;
- поиск оставленных вещей;
- отслеживание проникновения в запретные зоны;
- распознавание бесцельного блуждания (праздношатания);
- обнаружение быстрого передвижения [3].

Эти методы являются лишь некоторыми из возможных способов определения подозрительной активности и могут использоваться в различных комбинациях, чтобы обеспечить наиболее точное обнаружение угроз.

Мониторинг скопления людей. Один из способов определения подозрительной активности - это поиск скопления людей (например, рис. 1). Такое скопление может свидетельствовать о потенциальной угрозе безопасности, поэтому многие системы безопасности используют данную функцию в своей работе. Например, ситуационная видеоаналитика «ObjectVideo» [4] от компании «Avigilon» определяет скопление людей как одновременное присутствие определенного числа людей в зоне наблюдения в течение установленного времени. При этом можно настраивать параметры сканируемой зоны, максимальное число людей и продолжительность времени, которые считаются подозрительными.

Рисунок 1. Пример подозрительного скопления людей

Однако не всегда скопление людей является признаком подозрительной активности. Например, на крупных мероприятиях или в местах с большим скоплением людей, таких, как торговые центры, это может быть обычной ситуацией. Поэтому, помимо поиска скопления людей, системы безопасности также могут использовать другие методы для определения подозрительной активности, такие, как анализ поведения и звуковые датчики. Комбинация нескольких методов может повысить точность определения подозрительных действий и помочь предотвратить возможные угрозы для безопасности.

Учет количества входящих и выходящих людей. Другим методом определения подозрительной активности является использование счетчика входящих и выходящих людей. Этот инструмент (например, рис. 2) позволяет контролировать количество объектов, проходящих через заданную линию контроля в заданных направлениях. Направление и линия контроля могут быть настроены в соответствии с требованиями безопасности. Если количество входящих и выходящих людей не совпадает, это может указывать на наличие злоумышленника внутри защищенной зоны, который либо незаконно проник туда, либо не выходит из нее.

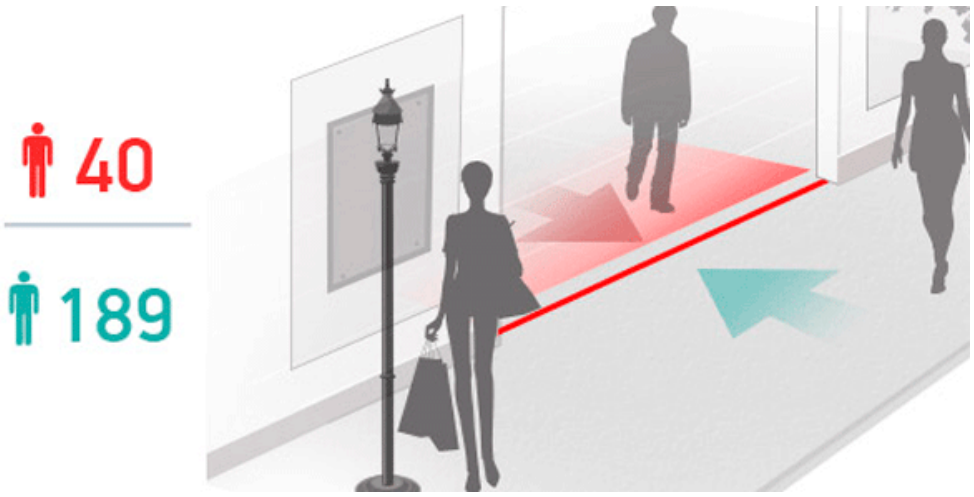


Рисунок 2. Пример счетчика входящих и выходящих людей

Поиск оставленных предметов – это еще один метод, применяемый в системах видеонаблюдения для повышения безопасности. Согласно официальному сайту компании Macroscop [5], данная функция может помочь уменьшить риски террористических актов и других опасных ситуаций, связанных с оставленными предметами. При использовании данного метода программа анализирует сканируемую зону и ищет объекты, оставленные в ней на заданный период времени. Если предмет оставлен неподвижно в течение заданного времени, система должна оповестить пользователя об этом событии. Хотя чаще всего оставленные предметы являются результатом забывчивости или потери, существует риск того, что предмет может быть опасным для окружающих. Поэтому быстрое обнаружение оставленных предметов является важным инструментом для обеспечения безопасности в общественных местах, таких, как аэропорты, транспортные узлы и другие места с большим скоплением людей.

Фиксация проникновения в запретную зону является одним из наиболее важных функций системы видеонаблюдения. В случае наличия строго охраняемой зоны, доступ в которую запрещен, метод фиксации проникновения (например, рис. 3) может стать ключевым элементом обеспечения безопасности. Согласно статье о современной видеоаналитике [6], этот метод работает следующим образом: при проникновении в запрещенную зону, размеры которой задаются пользователем, система автоматически фиксирует момент нарушения в базе данных и уведомляет администратора о произошедшем событии. Это позволяет оперативно принимать меры по предотвращению нежелательных последствий и обеспечивать максимальную безопасность.

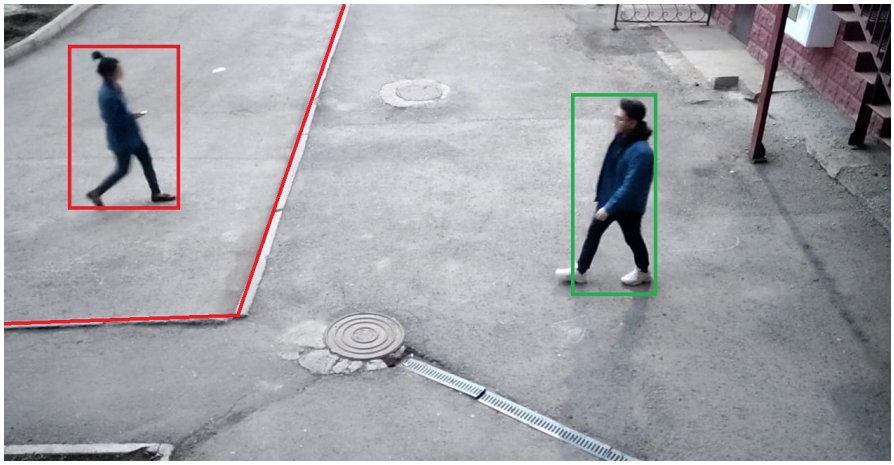

Рисунок 3. Пример проникновения в запретную зону

Определение праздношатания имеет большое значение в системах видеонаблюдения. Если сканируемая зона является защищенной, но при этом доступна для прохождения людей через нее, то метод определения праздношатания (например, рис. 4) может быть использован для повышения уровня безопасности. Он позволяет обнаруживать подозрительные действия людей, задерживающихся в контролируемой зоне на продолжительное время. Американская компания «IRISITY» [7] разработала систему видеоаналитики, которая способна определить праздношатание. Термин «праздношатание», или «Loitering» для англоязычных разработчиков, используется для обозначения нахождения человека в защищенной, но проходимой зоне на продолжительное время. Это может свидетельствовать о злоумышленных действиях или намерениях. Если человек просто проходит через защищенную зону, это не вызывает подозрений. Однако, если он задерживается в этой зоне на некоторое время, это может означать, что его действия направлены внутри этой зоны, и эти действия могут быть

потенциально опасными. Использование системы определения праздношатания может помочь увеличить эффективность мер безопасности и предотвратить возможные угрозы.

Рисунок 4. Пример определения праздношатания

Фиксирование быстрого передвижения. Хотя большинство людей ускоряют свое передвижение по различным причинам, например, спешат на работу или занимаются спортом, однако быстрое передвижение (например, рис. 5) может быть вызвано противоправными действиями, такими, как нападение, кража или скрытие с места преступления. Поэтому программное обеспечение использует метод фиксирования бега, который определяет, когда человек передвигается со скоростью выше определенного порога. Если такой случай происходит, то это событие фиксируется и отправляется уведомление администратору системы. Это позволяет оперативно реагировать на возможные противоправные действия и предотвращать их.

Рисунок 5. Пример определения бега

## 3. Результаты и обсуждение

Существуют программы для анализа подозрительной активности с помощью камер, каждая из которых имеет свои преимущества и недостатки. Для исследования были выбраны достаточно популярные программы.

Avigilon Control Center. Это программа, использующая технологию аналитики видео для обнаружения подозрительной активности [8]. ACC может определять нарушения безопасности, такие, как вторжение на территорию, проникновение в запретную зону и оставление предметов без присмотра.

Преимущества:

- Высокая точность анализа видео. Программа использует множество алгоритмов машинного обучения и компьютерного зрения, которые позволяют обнаруживать различные нарушения безопасности.
- Возможность настройки под конкретные потребности. Программа может быть настроена на определенный объект, такой, как здание, парковка или склад, что увеличивает ее эффективность и точность анализа.
- Работа в режиме реального времени. Программа обеспечивает быстрый и надежный анализ видео, что позволяет быстро реагировать на возможные угрозы безопасности.

Недостатки:

- Высокая стоимость. Программа является одной из самых дорогих на рынке, что может быть проблемой для небольших организаций или частных лиц.
- Высокая чувствительность к шуму и ложным срабатываниям. Программа может реагировать на нормальные действия людей, такие, как прохождение по дороге или оставление вещей на земле, что может приводить к ложным тревогам и трате времени на проверку каждого из них.
- Ограничение на количество камер. Каждая лицензия на программу позволяет использовать только ограниченное количество камер, что может быть недостаточным для больших объектов.

Senstar Symphony. Это программа, использующая технологии машинного обучения для анализа видео и обнаружения подозрительной активности, такой, как вторжение на территорию и оставление предметов без присмотра [9].

Преимущества:

- Высокая точность анализа видео. Программа использует множество алгоритмов машинного обучения и компьютерного зрения, которые позволяют обнаруживать различные нарушения безопасности.
- Возможность настройки под конкретные потребности. Программа может быть настроена на определенный объект, такой, как здание, парковка или склад, что увеличивает ее эффективность и точность анализа.
- Возможность предупреждения о возможной опасности на основе анализа данных. Программа анализирует данные о движении и поведении людей на видео, что позволяет определять возможные угрозы и предупреждать о них заранее.

Недостатки:

- Высокая стоимость. Программа является одной из самых дорогих на рынке, что может быть проблемой для небольших организаций или частных лиц.
- Требовательность к аппаратному обеспечению. Для работы программы требуется высокопроизводительное оборудование, что может быть дополнительной затратой.
- Нет возможности обработки видео в режиме реального времени. Программа требует предварительной обработки видео, что может занять время и увеличить время реакции на возможные угрозы безопасности.

Briefcam. Это программа, которая использует технологии машинного обучения для анализа видео и обнаружения подозрительной активности, такой, как изменения в окружающей среде, движения людей и автомобилей, а также оставленные предметы [10].

Преимущества:

- Возможность обработки большого объема видеоматериала за короткий промежуток времени.
- Использование технологии компьютерного зрения для обнаружения подозрительных действий.
- Поддержка работы с видео разного качества и разрешения.

Недостатки:

- Не всегда точно определяет подозрительную активность.
- Требует большого количества времени и ресурсов для обучения.
- Программа имеет высокую цену.

DeepCam. Это программа, использующая искусственный интеллект и машинное обучение для обнаружения подозрительной активности, такой, как кража или насилие. DeepCam также может обнаружить пропавших людей и предупреждать о пожарах [11].

Преимущества:

- Программа может обнаруживать определенные поведения, например, бег, падение и т.д., а также распознавать лица и автомобильные номера.
- Использование глубокого обучения (deep learning) позволяет программе обрабатывать и анализировать большое количество данных быстро и точно.
- Возможность обнаружения подозрительной активности в реальном времени.

Недостатки:

- Программа может работать только с видео с высоким разрешением и качеством изображения, что может быть проблемой в случае использования старых камер.
- Высокая стоимость программы.
- Требует мощных вычислительных ресурсов для работы.

Проанализировав множество существующих программ для анализа подозрительной активности с помощью камер видеонаблюдения, можно описать функции и характеристики, которые описали бы идеальную программу для анализа подозрительной активности. Идеальная программа должна включать в себя следующие функции и характеристики:

- Широкий спектр функций: программа должна иметь возможность обнаруживать различные виды подозрительной активности, такие, как движение, определение лиц, детектирование объектов, анализ трафика и т.д.
- Высокая точность и надежность: программа должна быть способна обеспечивать точный и надежный анализ видео, что позволяет быстро и точно определять подозрительные события.
- Работа в режиме реального времени: программа должна обеспечивать быстрый анализ видео, что позволяет быстро реагировать на возможные угрозы безопасности.
- Интеграция с другими системами безопасности: программа должна легко интегрироваться с другими системами безопасности, такими, как системы доступа и тревожной сигнализации, чтобы обеспечивать комплексную безопасность объекта.
- Дружественный интерфейс: программа должна иметь простой и понятный интерфейс, что позволяет быстро освоить ее использование и управление.
- Гибкая настройка: программа должна иметь возможность настройки под конкретные потребности пользователя, что позволяет получить наилучший результат анализа.
- Экономическая эффективность: программа должна иметь разумную цену, соответствующую ее функциональности и возможностям, и обеспечивать максимальную экономическую эффективность использования.
- Поддержка большого количества камер: программа должна позволять использовать большое количество камер, что обеспечивает широкий охват и возможность анализа различных зон на объекте.
- Облачное хранилище данных: программа должна предоставлять возможность хранения данных в облачном хранилище, что обеспечивает доступность данных и увеличивает их защищенность.

Кроме перечисленных характеристик и функций, важно также обратить внимание на следующие аспекты при выборе программы для анализа подозрительной активности:

- Система обработки данных: программа должна обеспечивать быструю и эффективную обработку данных для точного анализа видео и определения подозрительных событий.
- Система оповещения: программа должна иметь систему оповещения пользователя о подозрительных событиях, например, отправлять уведомления на мобильный телефон или электронную почту, чтобы быстро реагировать на угрозы.
- Автоматическое определение категории события: программа должна иметь возможность автоматического определения категории подозрительного события, например, различать между воровством и нападением, чтобы обеспечить точную реакцию.
- Система аналитики: программа должна иметь возможность анализировать и отслеживать поведение людей и объектов на длительном периоде времени, чтобы обнаружить повторяющиеся события и предотвратить возможные угрозы.
- Гибкость использования: программа должна быть гибкой в использовании, что позволяет ее применять на разных объектах и в разных условиях.
- Поддержка обучения программы: программа должна предоставлять возможность обучения программы на конкретные условия объекта и поведение людей, что позволяет улучшить точность анализа и определения подозрительных событий.
- Техническая поддержка: программа должна иметь хорошую техническую поддержку со стороны производителя, что обеспечивает быстрое решение возможных проблем при использовании программы.
- Внедрение искусственного интеллекта и машинного обучения: это позволит программам быстрее и точнее обнаруживать подозрительные события и даже предсказывать возможные угрозы на основе данных об аномальном поведении людей и объектов.
- Разработка мобильных приложений: разработка мобильных приложений позволит пользователям получать быстрое уведомление об подозрительных событиях и контролировать безопасность своего объекта из любой точки мира.

В целом программы для анализа подозрительной активности с помощью камер видеонаблюдения представляют собой важный инструмент для обеспечения безопасности в обществе. Каждая программа имеет свои преимущества и недостатки, которые могут влиять на их эффективность и полезность в конкретной ситуации. Поэтому важно выбирать программу, которая наилучшим образом соответствует потребностям и задачам организации.

## 4. Выводы

В заключение можно сказать, что использование камер видеонаблюдения и программ для анализа подозрительной активности является важным компонентом в системах обеспечения безопасности на объектах различного назначения. Современные технологии позволяют автоматически обнаруживать подозрительную активность на основе анализа видеопотока и реагировать на нее в режиме реального времени.

Однако необходимо учитывать, что любые технологии имеют свои ограничения и не могут заменить руководящий персонал в процессе обеспечения безопасности. Поэтому необходимо использовать камеры видеонаблюдения и программы для анализа подозрительной активности в сочетании с квалифицированным персоналом для достижения максимальной эффективности в обеспечении безопасности объектов.

Использование технологий для обеспечения безопасности является непрерывным процессом, который требует постоянного совершенствования и адаптации к новым угрозам и вызовам. Поэтому необходимо продолжать исследования и разработки в области программ для анализа подозрительной активности и использования камер видеонаблюдения для обеспечения безопасности объектов.

## Список литературы

1. Дмитриев Д.В. Толковый словарь русского языка Дмитриева, 2003 г. - 228 с.
2. SPOT (Screening of Passengers by Observation Techniques. [Электронный ресурс]. URL: https://www.dhs.gov/publication/screening-passengers-observation-techniques-spot-program#:~:text=The%20Screening%20of%20Passengers%20by,potential%20transportation%20security%20risks%20by (дата обращения 12.12.2022).
3. Ситуационная видеоаналитика SECUROS. [Электронный ресурс]. URL: https://iss.ru/pub/uploads/fb0506c2-89ff-4b29-93fb-219250699fc4/securos-computer-vision-overview-ru.pdf (дата обращения 13.12.2022).
4. ObjectVideo Labs – Video Analytics and Computer Vision. [Электронный ресурс]. URL: https://objectvideolabs.com/ (дата обращения 14.12.2022).
5. Детектор оставленных предметов Macroscop. [Электронный ресурс]. URL: https://macroscop.com/produkty/programma-dlya-ip-kamer/detektor-ostavlennyh-predmetov (дата обращения 13.12.2022).
6. Видеоаналитика: термины, сферы применения, технологии Video Content Analysis. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Видеоаналитика_(термины,_сферы_применения,_технологии)/ (дата обращения 14.12.2022).
7. Irisity - Security beyond human intelligence. [Электронный ресурс]. URL: https://irisity.com/ (дата обращения 15.12.2022).
8. Products - Avigilon [Электронный ресурс]. URL: https://www.avigilon.com/products (дата обращения 03.02.2023).
9. Senstar Symphony Common Operating Platform [Электронный ресурс]. URL: https://senstar.com/products/video-management/senstar-symphony-common-operating-platform/ (дата обращения 10.02.2023).
10. VIDEO ANALYTICS INNOVATION UNLEASHED [Электронный ресурс] URL: https://www.briefcam.com/ (дата обращения 13.02.2023).
11. AI Powered SmartCam [Электронный ресурс] URL: https://wirakom.com/DeepCAM (дата обращения 28.02.2023).

## Күдікті әрекетті анықтау принциптері және бейнебақылау камераларының көмегімен күдікті әрекетті талдау бағдарламалары

**А.Б. Рустемов, Б.А. Кузенбаев**
*А. Байтұрсынов атындағы Қостанай өңірлік университеті, Қостанай, Қазақстан*

**Аңдатпа.** Ұсынылып отырған мақалада адам логикасы мен психологиясы тұрғысынан күдікті әрекетті анықтау принциптері талқыланады, сондай-ақ бейнебақылау камералары арқылы күдікті әрекетті талдауға арналған қолданыстағы бағдарламалар зерттеледі. Адамдардың көп жиналуы, жылдам қозғалуы, қорғалатын аумаққа және қараусыз қалған заттарға ену сияқты күдікті әрекеттің негізгі түрлері, сондай-ақ оларды анықтауға болатын әдістер мен құралдар қарастырылады. Қолданыстағы бағдарламаларды зерделеу бейнебақылау арқылы күдікті әрекеттерді талдауға арналған танымал бағдарламалардың артықшылықтары мен кемшіліктеріне тоқталады, соның ішінде осы бағытта басқа бағдарламалармен бәсекелесе алатын бағдарлама тұжырымдамасын талқылау, инновацияларды енгізу, бәсекелестердің артықшылықтарын пайдалану және оларды болдырмау. бәсекелестердің кемшіліктері.

**Түйін сөздер:** күдікті әрекет, бейнебақылау камералары, адам мінез-құлқын талдау, қауіпсіздік, машиналық оқыту.

## Principles for detecting suspicious activity and programs for analyzing suspicious activity using CCTV cameras

**A. Rustemov, B. Kuzenbaev**
*A.Baitursynov Kostanay Regional University, Kostanay, Kazakhstan*

**Abstract.** The proposed article discusses the principles of detecting suspicious activity from the point of view of human logic and psychology, and also explores existing programs for analyzing suspicious activity using CCTV cameras. The main types of suspicious activity are considered, such as crowding, fast movement, penetration into a protected area and things left unattended, as well as methods and tools that can be used to detect them. The study of existing programs touches on the advantages and disadvantages of popular programs for analyzing suspicious activity through video surveillance, including discussing the concept of a program that could compete with other programs in this direction, introducing innovations, using the advantages of competitors and avoiding the disadvantages of rivals.

**Keywords:** suspicious activity, video surveillance cameras, human behavior analysis, security, machine learning.

### References

1. Dmitriev D.V. Explanatory dictionary of the Russian language Dmitriev, 2003, - 228 p.
2. SPOT (Screening of Passengers by Observation Techniques. [Electronic resource]. URL: https://www.dhs.gov/publication/screening-passengers-observation-techniques-spot-program#:~:text=The%20Screening%20of %20Passengers%20by,potential%20transportation%20security%20risks%20by (accessed 12/12/2022)
3. Situational video analytics SECUROS. [Electronic resource]. URL: https://iss.ru/pub/uploads/fb0506c2-89ff-4b29-93fb-219250699fc4/securos-computer-vision-overview-ru.pdf (Accessed 13.12.2022)
4. ObjectVideo Labs - Video Analytics and Computer Vision. [Electronic resource]. URL: https://objectvideolabs.com/ (accessed 12/14/2022)
5. Detector of abandoned objects Macroscop. [Electronic resource]. URL: https://macroscop.com/produkty/programma-dlya-ip-kamer/detektor-ostavlennyh-predmetov (accessed 12/13/2022)
6. Video analytics terms, scopes, technologies Video Content Analysis. [Electronic resource]. URL: https://www.tadviser.ru/index.php/Article: Video analytics_(terms,_fields_of_application,_technologies)/ (accessed 12/14/2022)
7. Irisity - Security beyond human intelligence. [Electronic resource]. URL: https://irisity.com/ (accessed 12/15/2022)
8. Products - Avigilon [Electronic resource]. URL: https://www.avigilon.com/products (accessed 02/03/2023)
9. Senstar Symphony Common Operating Platform [Electronic resource]. URL: https://senstar.com/products/video-management/senstar-symphony-common-operating-platform/ (accessed February 10, 2023)
10. VIDEO ANALYTICS INNOVATION UNLEASHED [Electronic resource] URL: https://www.briefcam .com/ (accessed 02/13/2023)
11. AI Powered SmartCam [Electronic resource] URL: https://wirakom.com/DeepCAM (accessed 02/28/2023)

### Сведения об авторах:

***А.Б. Рустемов*** – магистрант, Костанайский региональный университет имени А. Байтурсынова, ул. Абая, 28, Костанай, Казахстан.

***Б.А. Кузенбаев*** – PhD, заведующий кафедрой, Костанайский региональный университет имени А. Байтурсынова, ул. Абая, 28, Костанай, Казахстан.

***А.Б. Рустемов*** – магистрант, А. Байтұрсынов атындағы Қостанай өңірлік университеті, Абай көш., 28, Қостанай, Қазақстан.

***Күзенбаев Б.А***. – PhD докторы, кафедрасының меңгерушісі, А. Байтұрсынов атындағы Қостанай өңірлік университеті, Абай көш., 28, Қостанай, Қазақстан.

***Rustemov A. B.*** – master's student, A.Baitursynov Kostanay Regional University, 28 Abay str., Kostanay, Kazakhstan.

***Kuzenbaev B.A***. – PhD, Head of the Department, A.Baitursynov Kostanay Regional University, 28 Abay str., Kostanay, Kazakhstan.