DOI 10.37882/2223-2966.2023.08.02

ВЗАИМОСВЯЗЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ВИДЕОНАБЛЮДЕНИЯ В СИСТЕМЕ БЕЗОПАСНОСТИ

THE RELATIONSHIP OF ARTIFICIAL INTELLIGENCE AND VIDEO SURVEILLANCE IN THE SECURITY SYSTEM

D. Andryushenkov
N. Hadi
N. Ushkova
K. Bolotin

Summary. The article will consider examples of integrating artificial intelligence into a video surveillance system, conduct a system analysis, show the process of their interaction, identify weaknesses, and also illustrate their inextricable link with security. A situation will be presented in which there are any threats to people and it will be shown which algorithms the system uses. During the execution, an intelligent system was developed that is able to analyze the actions on the video recordings and detect suspicious movements that precede the commission of shoplifting. The proposed system can analyze movement according to two main classifications: natural movement and suspicious movement (with the determination of the percentage of each of them). Certain practical conclusions will also be made, which, perhaps, can improve the security system and take a fresh look at emerging threats.

Keywords: artificial intelligence, video surveillance, threats, video analytics, system analysis, security, people, neural network, algorithms.

Андрюшенков Дмитрий Геннадьевич
Аспирант, МИРЭА — Российский технологический университет (РТУ МИРЭА).
andryushenkov@mirea.ru
Хади Намир Мохамед
Аспирант, МИРЭА — Российский технологический университет (РТУ МИРЭА).
hadi@mirea.ru
Ушкова Надежда Николаевна
Аспирант, МИРЭА — Российский технологический университет (РТУ МИРЭА).
ushkova@mirea.ru
Болотин Кирилл Викторович
Аспирант, МИРЭА — Российский технологический университет» (РТУ МИРЭА)
bolotin@mirea.ru

Аннотация. В статье будут рассмотрены примеры интеграции искусственного интеллекта в систему видеонаблюдения, проведен системный анализ, показан процесс их взаимодействия, выявлены слабые стороны, а также будет проиллюстрирована их неразрывная связь с безопасностью. Будет представлена ситуация, в которой присутствуют какие-либо угрозы для людей и будет показано, какие алгоритмы применяет система. В ходе выполнения была разработана интеллектуальная система, способная анализировать действия на видеозаписях и обнаруживать подозрительные движения, предшествующие совершению магазинных краж. Предлагаемая система может анализировать движение по двум основным классификациям: естественное движение и подозрительное движение (с определением процентной доли каждого из них). Также будут сделаны определенные практические выводы, которые, возможно, могут позволить улучшить систему безопасности и по-новому взглянуть на возникающие угрозы.

Ключевые слова: искусственный интеллект, видеонаблюдение, угрозы, видеоаналитика, системный анализ, безопасность, люди, нейронная сеть, алгоритмы.

Введение

Взаимосвязь искусственного интеллекта и видеонаблюдения в системе безопасности достаточно интересный предмет научной дискуссии. Основные споры ведутся в вопросе рассмотрения видеонаблюдения как обычной системы фиксации происходящего и более совершенной системы на основе искусственного интеллекта, которая способна заменить в работе человека и повысить показатели полезности. С точки зрения взаимодействия видеонаблюдения и искусственного интеллекта можно рассмотреть все возможности по совместной работе, оценить их влияние на жизнь человека и его безопасность, а также дать оценку эффективности работы системы и рассмотреть угрозы и уязвимости. Исходя из подобных рассуждений, нетрудно заметить, что теория этого вопроса обладает большой ценностью. Из теории, в свою очередь, следуют некоторые выводы, которые обладают важным практическим значением.

Определение системы видеонаблюдения

Обсуждение начинается с постановки вопроса, что в первую очередь представляет собой система видеонаблюдения. Ответ на этот вопрос в настоящее время имеет огромное множество различных вариантов, которые являются актуальными по мере использования системы.

На первый взгляд может показаться, что система видеонаблюдения представляет собой монитор и видеокамеры, которые фиксируют происходящее и подобная концепция достаточно проста. В этом подходе

видеонаблюдение является полностью подконтрольной человеку системой, которая выполняет свойственные ей действия по фиксации видео и никак не сможет самостоятельно повлиять на предотвращение критических ситуаций, которые могут угрожать человеку или любому другому объекту. Предполагается, что видеонаблюдение может работать в комплексе с другими составляющими системы безопасности и быть более эффективной, но нужно понимать, что ключевым механизмом в этой системе все равно является человек, без которого данная система потеряет свою актуальность и уж точно не будет эффективной. Но люди несовершенны, зачастую они несовершенны намеренно, и когда ключевой механизм системы целенаправленно пытается злоупотребить положением и нарушить законы Российской Федерации. Не стоит надеяться, что данная ситуация минует большинство предприятий, как, например, служба безопасности «Газпромбанка», где злоумышленники в сговоре с охраной заведения украли из средств банка огромную сумму денег, а «Газпромбанк» занимает лидирующие позиции по размеру активов. И таких примеров огромное количество. Подобные истории могут надвинуть на мысль ужаса и бесполезности систем безопасности, но кроме воровства, мошенничества, саботажа и многих других злоупотреблений, существуют и другие направления, в которых видеонаблюдение играет особо важную роль. Может показаться, что раз угроза возникла, а система безопасности справилась с ней, то совершенствование комплекса не актуально, но, человек, живя в эпоху цифровых технологий и искусственного интеллекта, должен понимать, что угрозы с каждым днем представляют все большую опасность, и с темпами их развития должны совершенствоваться системы безопасности, которым необходимо работать на максимум своей эффективности, чтобы оправдывать себя. Без внедрения в системы видеонаблюдения интеллектуальной видеоаналитики никогда не будет возможным поймать преступника, и системы безопасности устареют [1].

Взаимосвязь видеонаблюдения и искусственного интеллекта

Далее предлагается рассмотреть вопрос о возможности взаимосвязи видеонаблюдения и искусственного интеллекта. Необходимо провести системный анализ. Системный анализ видеонаблюдения — это процесс анализа системы видеонаблюдения с целью определения ее эффективности и возможности улучшения ее функциональности. В рамках системного анализа видеонаблюдения рассматриваются несколько важных аспектов, таких как определение ключевых компонентов системы, разработка стратегий расположения камер наблюдения на объекте и оценка методов обработки и анализа видеоинформации. Эти три компонента играют важную роль в построении комплексной системы безопасности. Расположение видеокамер на объекте играет одну из ключевых ролей в построении системы безопасности, ведь без правильного расположения камер дальнейшие действия будут лишены всякого смысла, система не будет работать должным образом. Как только камеры будут расположены по разработанной стратегии, в силу вступают два следующих не менее важных аспекта: определение ключевых компонентов системы и оценка методов обработки и анализа видеоинформации. В этом случае делается вывод о неизбежной интеграции искусственного интеллекта и видеонаблюдения. Данная интеграция представляет собой использование компьютерного зрения и аналитики данных для улучшения возможностей видеонаблюдения. Например, при помощи искусственного интеллекта можно обнаруживать незаконные действия, такие как магазинные кражи.

Операции по краже в магазине и их планирование являются одним из самых сложных задач классификации, поскольку люди-наблюдатели внутри центра управления должны следить за всеми перемещениями посетителей, которые совершают покупки внутри магазина в режиме реального времени. В большинстве случаев человек-наблюдатель не может распознать кражи, и это приводит к неопределенности того, что действия, совершаемые ворами, могут привести к различным исходам событий. Следовательно, одна из причин неспособности наблюдателя-человека идентифицировать операции по краже является предварительное планирование группой воров, цель которых состоит в том, чтобы отвлечь наблюдателей, и, таким образом, процесс кражи происходит без возможности человека-наблюдателя идентифицировать её. В качестве примера можно привести исследование [2], которое основывается на определении начала времени, когда началось подозрительное перемещение, и времени, когда подозрительное перемещение закончилось. Пример видео-сегментации представлен на рис. 1.

Также интеграция искусственного интеллекта может помочь в определении потенциальных опасностей, например, автомобилисты, которые ездят с нарушением правил дорожного движения. Использование искусственного интеллекта позволяет сделать видеонаблюдение более эффективным, уменьшить количество ошибок и оптимизировать процессы. К примеру, можно использовать алгоритмы глубокого обучения [3] для автоматического распознавания лиц и определения объектов на видео. Также интеграция искусственного интеллекта и видеонаблюдения позволяет улучшить аналитику и обработку данных, что дает возможность проводить более эффективный мониторинг и принимать более обоснованные решения на основе данных.

Таким образом, можно сделать вывод, что взаимосвязь искусственного интеллекта и видеонаблюдения превращается в важный инструмент системы безопас-

Рис. 1. Сегментация видео с использованием моментов, полученных методом сегмента поведения до совершения преступления [Guillermo A. Martínez-Mascorro, 2021]

ности любого предприятия. Это положительно влияет на функциональную составляющую комплекса, которая самостоятельно способна оценивать обстановку и принимать решения без участия оператора при помощи интеллектуальной видеоаналитики.

Связь искусственного интеллекта и человека

Связь искусственного интеллекта и человека заключается в том, что искусственный интеллект создается и управляется людьми. Они задают параметры, по которым система будет функционировать, а также обучают ее на примерах. С другой стороны, искусственный интеллект может помочь человеку в различных областях, упрощая работу и повышая производительность. Например, в медицине искусственный интеллект может помочь с диагнозом и лечением пациентов, в бизнесе — с прогнозированием продаж и оптимизацией процессов. Однако возможно появление определенных проблем, таких как замещение работ человека машинами и возможность использования искусственного интеллекта в целях контроля и манипуляции. Поэтому необходимо установить правила этического использования искусственного интеллекта. Если размышлять на тему дальнейшего взаимодействия человека и искусственного интеллекта, то можно сделать два вывода, либо в будущем наш мир превратится во что-то сказочное, по типу голливудских фильмов, где искусственный интеллект правит миром, либо же в какой-то момент интеграция может приостановиться на том уровне, где человеку все еще будет возможно контролировать систему. Хотя искусственный интеллект уже играет значительную роль в разных сферах нашей жизни, будущее обещает еще большее взаимодействие между искусственным интеллектом и человечеством. Одной из наиболее важных областей будущего взаимодействия искусственным интеллектом и людей является развитие более человеческой и гибкой ИИ. Это включает в себя улучшение навыков машинного обучения, а также развитие способностей искусственного интеллекта к адаптации к новым ситуациям и изменению своих действий в соответствии с изменяющимся окружением. Кроме того, ИИ может играть ключевую роль в таких областях, как медицина и экология. Например, ИИ может помочь докторам в диагностировании заболеваний и выборе более эффективных лекарственных средств, а также помочь врачам улучшить планирование лечения. В экологии, ИИ может помочь в заботе о природных ресурсах и борьбе с изменением климата. Однако, улучшение технологий в области ИИ может вызвать опасения и вызывать критику, особенно в контексте безопасности и конфиденциальности. Быстрое развитие ИИ может стать причиной возникновения новых этических и социальных проблем, которые мы еще не можем предугадать. Так или иначе, будущее взаимодействия ИИ и человечества обещает быть увлекательным и разнообразным, долгое время продолжая вызывать немало вопросов и дилемм [4].

Практические ситуации с использованием интеллектуальных систем видеонаблюдения

В предлагаемой системе видеонаблюдения, основанной на нескольких видеороликах, включающих кражи, была использована концепция, созданная в исследовании [2], но с большим улучшением работы с используемым набором данных и моментами времени, и целью этого является возможность получения наивысшей точности, чем полученная в исследовании [2]. Таким образом, в данной работе используется набор данных UCF-Crime [5] для анализа подозрительного поведения во время совершения преступных действий, связанных с кражами в магазинах. Набор данных состоит из 1900 видеозаписей наблюдений и содержит около 129 часов видеоклипов. Видео отображаются с разрешением 320x240 пикселей. Набор данных включает сценарии, сгруппированные по 13 категориям, таким как: жестокое обращение, кража со взломом, взрыв и пр. Были извлечены образцы из категорий «ограбление магазина» и «обычные» из набора данных UCF-Crime.

Что касается видеозаписей краж, видеозаписи были разделены на три разных периода следующим образом:

— В тот момент, когда появился вор, что было его естественным движением.

— В тот момент, когда для вора началось подозрительное движение.
— В тот момент, когда вор совершил кражу.
— В тот момент, когда кража была завершена.
— В тот момент, когда движение вернулось в норму.

Согласно этому разделению, будут извлекаться периоды как для нормального движения, так и для ненормального движения из видеозаписей кражи.

Таким образом, методология сбора набора данных основывалась на использовании видеозаписей процесса кражи для выделения моментов, когда движение было нормальным, и моментов, когда движение было ненормальным, и этот процесс поможет нейронной сети точно идентифицировать странное движение и внезапное изменение, которое произошло. На рис. 2 представлена сегментация и сбор визуальных образов из видео, где происходит ограбление.

Было использовано несколько видеороликов из категории «естественное видео», поскольку были отобраны все видеоролики, которые были записаны с помощью камер наблюдения в магазинах и торговых центрах. Количество видеороликов о краже, которые были использованы для обучения нейронной сети, равняется 104, а количество видеороликов, где было естественное поведение –— 109. Каждый период для конкретного случая был разделен на несколько частей, чтобы повысить точность нейронной сети в определении деталей движения, поскольку движение каждый раз делилось на 400 кадров. Нейронная сеть более точно запоминает детали

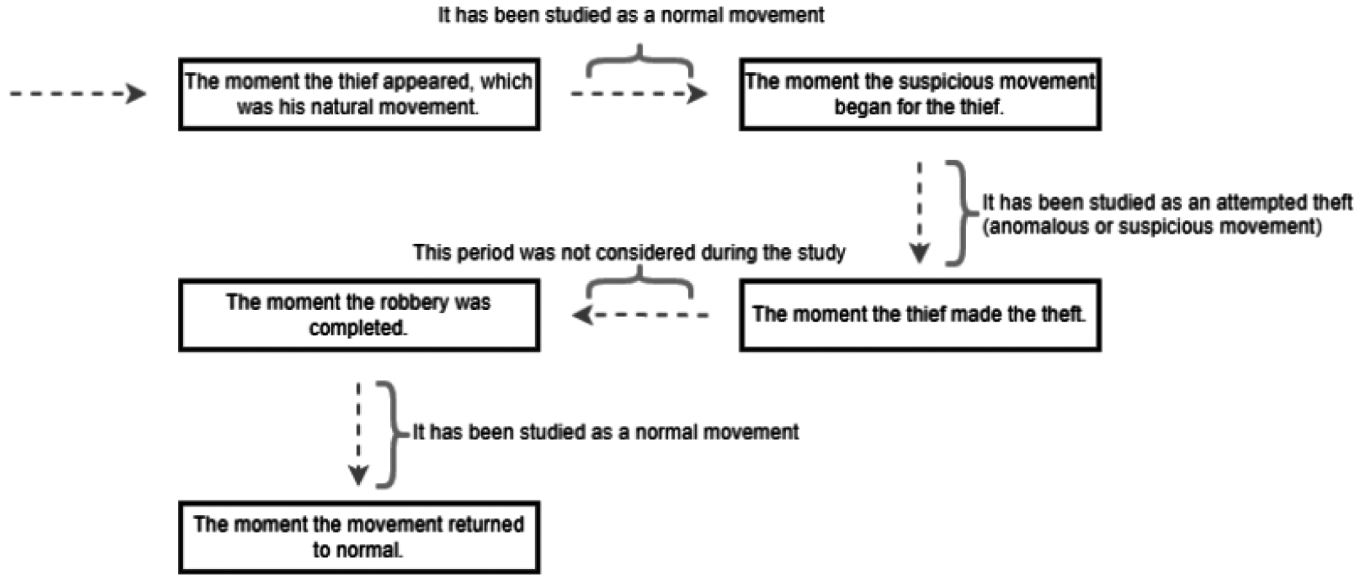

Рис. 2. Сегментация и сбор визуальных моментов из видеороликов, которые включают случаи ограбления

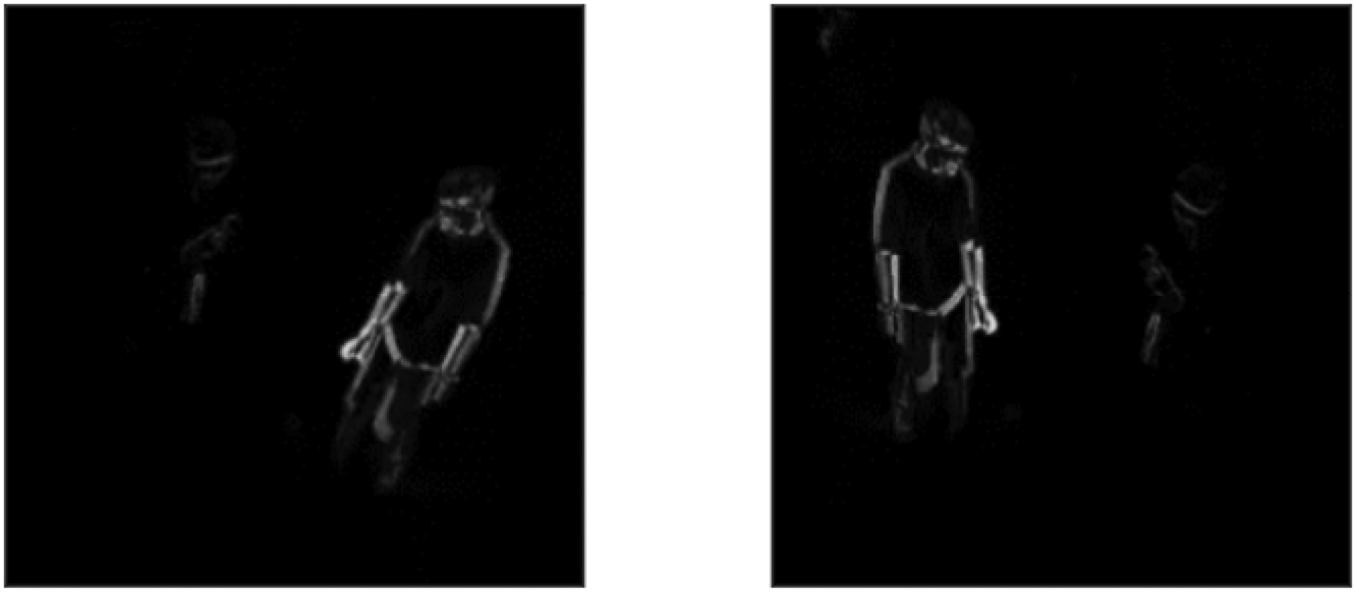

Рис. 3. Пример аугментации данных из видео

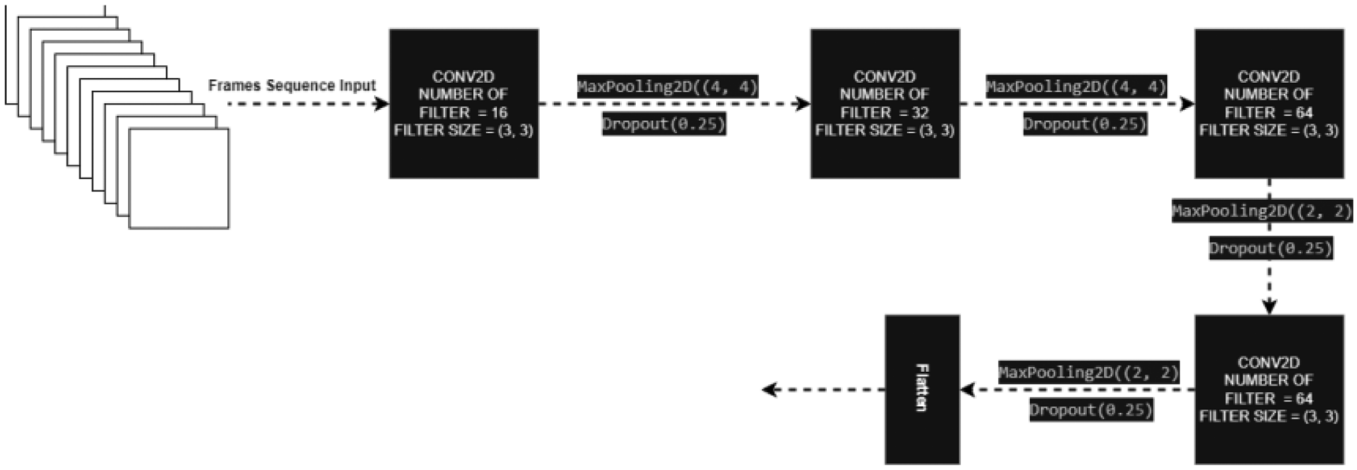

Рис. 4. Архитектура сверточной нейронной сети

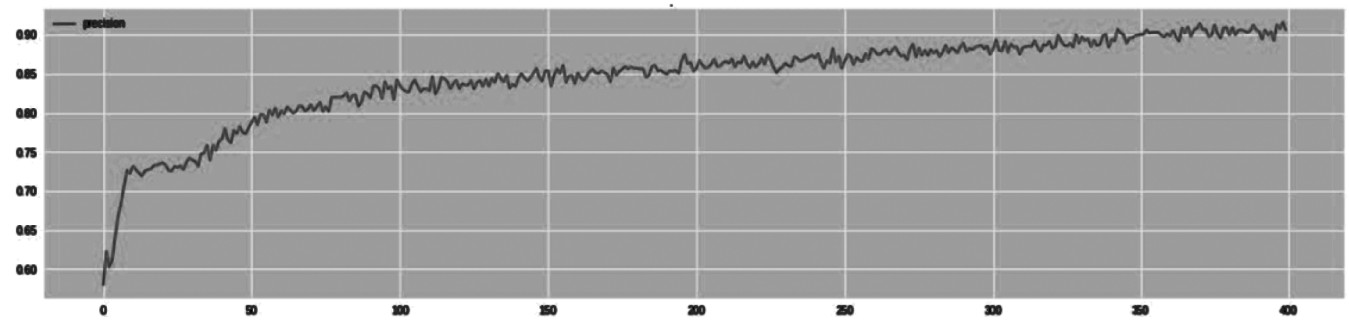

Рис. 5. Диаграмма увеличения точности на этапе обучения

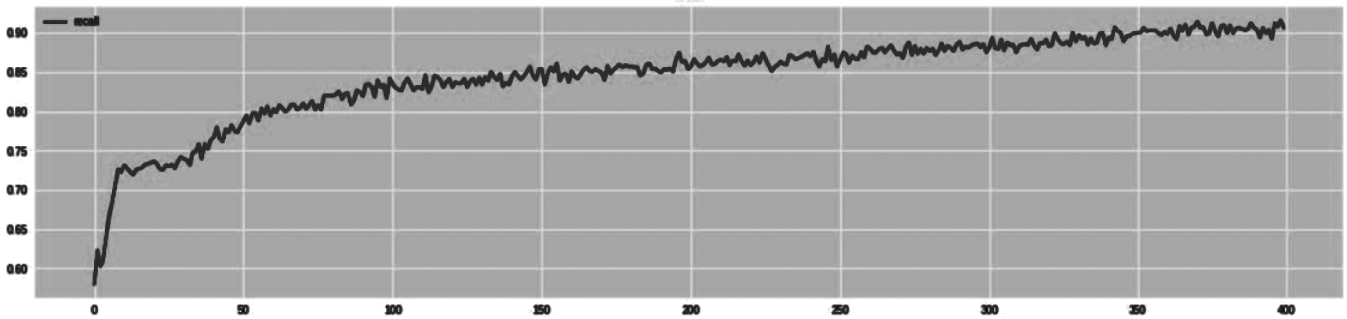

Рис. 6. Диаграмма увеличения отзыва на этапе обучения

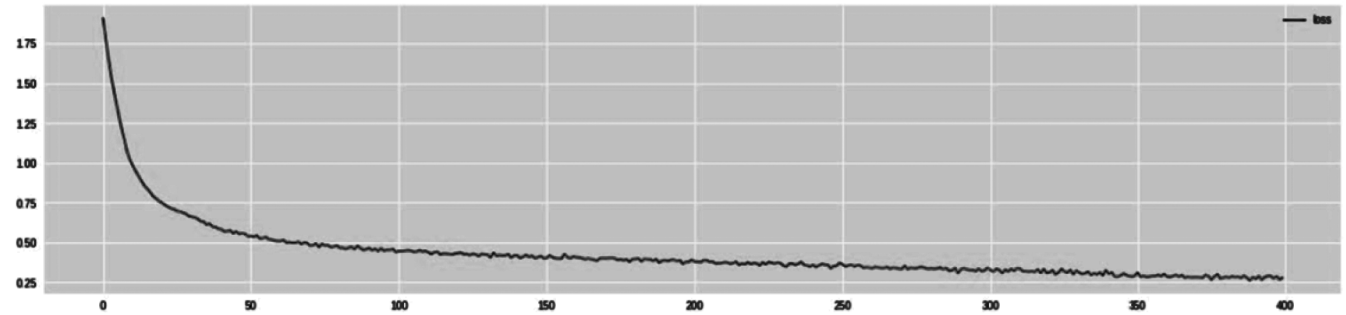

Рис. 7. Диаграмма уменьшения значения потерь на этапе обучения

подозрительного движения и естественного перемещения. Количество частей, которые были получены после изучения движения через каждые 400 символов, достигло 289 видеоклипов, представляющих подозрительное движение (движение, предшествующее краже), и 320 видеоклипов, представляющих естественное движение. На рис. 3 представлено аугментация данных из видео.

Поскольку система анализирует передвижение, обнаруживая намерение совершить кражу внутри магази-

на, то необходимо обобщить возможности нейронной сети, чтобы иметь возможность анализировать передвижение людей в контролируемой зоне, было предложено использовать аугментацию данных для генерации более значительного количества видеороликов, включающих клоны людей в контролируемой зоне с изменением направления движения по горизонтали, а также с использованием угла наклона в 30 градусов. Для данного случая было сгенерировано множество дополнительных ситуаций перемещения людей с изменением направления и угла наклона.

На рис. 4 представлена архитектура сверточной нейронной сети, которая использовалась для извлечения свойств из фреймов.

Данная сверточная нейронная сеть используется для изучения характеристик каждого кадра. Она состоит из нескольких слоев в дополнение к определению характеристик каждого из используемых слоев.

В качестве результата приведены диаграммы показывающие увеличение точности и отзыва на этапе обучения и уменьшение значения потерь.

Заключение

Рассмотрение взаимосвязи искусственного интеллекта и видеонаблюдения оказалось очень полезным изысканием. В отдельности видеонаблюдение представляет собой примитивную систему видео фиксации, которая в скором времени потеряет свою актуальность. Искусственный интеллект в нашем мире является свежим и новым решением, которое способно превознести функциональность технической системы. Предложенная модель обеспечивает высокую вероятность обнаружения кражи (обнаружение подозрительного перемещения). Есть возможность расширить систему в будущем, изучив разведывательные данные групп и выявлять людей, планирующих кражу. Идентификация таких преступных групп помогает службам безопасности повысить точность отслеживания и мониторинга.

ЛИТЕРАТУРА

1. Могилин К.А., Карманова И.А. Интеллектуальные системы видеонаблюдения в комплексах безопасности// Известия ТулГу. Технические науки. 2020. Вып. 3. С. 89–92.
2. Guillermo A. Martínez-Mascorro, José R. Abreu-Pederzini, José C. Ortiz-Bayliss, Angel Garcia-Collantes, Hugo Terashima-Marín Criminal Intention Detection at Early Stages of 362 //[Electronic resource] URL: https://udimundus.udima.es/bitstream/handle/20.500.12226/736/articulo%20monterrey.pdf?sequence=1&isAllowed=y (access data — 28.05.2023)
3. Кручинин А.Ю., Колмыков Д.В., Галивом Р.Р. Алгоритм распознавания ситуаций в распределенной системе видеонаблюдения// Программные продукты и системы/ Научная статья. 2018. Т. 31. № 2. С. 1–5.
4. Интеллектуальная видеоаналитика, как сделать умное наблюдение с видеоаналитикой (от бесплатной до нейросетевой) // [Электронный ресурс] URL: https://securityrussia.com/blog/videoanalitika.html?ysclid=libp2osoxg961424378/ (дата обращения — 31.05.2023)
5. Sultani W., Chen C., Shah M. Real-world anomaly detection in surveillance videos [Electronic resource]. URL: https://arxiv.org/pdf/1801.04264.pdf (access data: 31.05.2023)