Тахмасиб Дадашев

СОВРЕМЕННЫЕ ПЛАТФОРМЫ ВИДЕОБЕЗОПАСНОСТИ

ISBN 978-609-95007-1-3

Содержание

www.5ci.net

Penki kontinentai GRUPĖ

Группа предприятий

PENKI KONTINENTAI

Мы объединяем континенты

Группа предприятий PENKI KONTINENTAI является одной из самых передовых корпораций, работающих в сфере банковских технологий, инновационных платежных решений, оптоволоконного интернета, IPTV, телефонии и Интернета Вещей. Решения и услуги группы компаний зарекомендовали себя в 80 странах мира.

Предисловие

Внедрение новейших технологий ныне становится повсеместным: новейшие технические принципы и решения становятся неотъемлемой частью повседневной жизни человека, направляя, помогая и наблюдая за нами. Благодаря использованию всевозможных мобильных устройств и систем самообслуживания технологии предоставления услуг дошли до такой стадии развития, когда у представителей бизнеса имеется возможность получить практически любую исчерпывающую информацию о своём клиенте. Парадоксально, но этот воплощенный в жизнь принцип «Знай своего клиента» не удовлетворил, а, напротив, лишь подчеркнул потребность поставщика услуги в получении большего количества данных о потребителе.

Эта книга может служить кратким справочником по вопросам видеонаблюдения, видеобезопасности и защиты данных в ходе проведения банковских операций, а также своеобразной авторской попыткой выявить тенденции, которые будут определять будущее банковских технологий в ближайшие годы.

Активное участие в подготовке данной книги приняли специалисты группы компаний Penki Kontinentai (Литва), на протяжении 25 лет успешно работающей в области телекоммуникаций, технологий для финансового и банковского секторов, в частности, для защиты устройств самообслуживания. BS/2 – компания, входящая в эту группу, – специализируется на предоставлении аутсорсинговых услуг для банков и предприятий розничной торговли, разработке программного обеспечения и поставках банковского оборудования. BS/2 является эксклюзивным партнером немецкого концерна Diebold Nixdorf – крупнейшего мирового производителя оборудования и поставщика готовых решений для финансовых учреждений и других организаций.

Решения и услуги компании BS/2 широко известны на мировом рынке, её продукция поставляется в 80 стран мира. В их числе — семейство программных продуктов *«.iQ»*. Это — развитый комплекс решений, обеспечивающих безопасность банковских устройств самообслуживания, повышение эффективности их работы и снижение стоимости владения этим дорогостоящим оборудованием.

Так, программное решение *ATMeye.iQ*, которое предназначено для видеомониторинга банкоматов и других устройств самообслуживания, позволяет составлять подробные отчёты о производимых на терминалах действиях с предоставлением фото- и видеоматериалов по транзакционным и иным событиям, а также давать тревожные уведомления для отвечающего за безопасность персонала в режиме реального времени. Таким образом реализуются принципы проактивной защиты для наиболее чувствительной части банковской инфраструктуры; обеспечивается надёжное видеонаблюдение за действиями пользователя устройства самообслуживания, снижаются риски, связанные с мошенничеством и вандализмом.

В отличие от фундаментального труда Владо Дамьяновски «Библия видеонаблюдения» [1], в основном, посвящённого специализированному аппаратному обеспечению, в этой книге больше внимания уделяется именно программному обеспечению для информационной и видеобезопасности.

Ещё 70 лет назад британский писатель Джордж Оруэлл в романе-антиутопии «1984» [5] впервые описал внедрение технологий видеонаблюдения в обществе всеобщего контроля. Читатели смогут оценить его футуристическое видение по эпиграфам к отдельным разделам этой книги.

Введение. Базовые концепции и технологии видеонаблюдения и видеобезопасности

«Телекран работал на прием и на передачу… Конечно, никто не знал, наблюдают ли за ним в данную минуту или нет…»

Дж. Оруэлл, «1984»

Задача *видеонаблюдения* предусматривает визуальный контроль выделенной области пространства посредством одной или нескольких видеокамер, обеспечивающий сохранение и просмотр цифровых видеоданных, а также постоянную оценку состояния контролируемой территории, выявляя так называемые *«тревожные события»* по изменениям в наблюдаемой обстановке.

Исторически основными функциями системы видеонаблюдения считаются вывод информации на пункт контроля и запись в архив. Большинство производителей платформ охранного телевидения (*closed-circuit television; CCTV*) ориентированы именно на такую модель работы.

Основной тенденцией в развитии систем видеонаблюдения ныне становится переход от аналогового способа получения (аналоговые камеры), отображения (телевизоры) и хранения видео (видеокассеты) к цифровому (IP-камеры, компьютерные мониторы и цифровые базы данных). Поэтому теперь в построении и эффективной эксплуатации систем видеонаблюдения важную роль играют *технологии сжатия, хранения, поиска и передачи цифрового видео.*

Автоматические и автоматизированные системы видеонаблюдения являются одной из ключевых составляющих нынешних комплексов безопасности. Современные распределенные

системы видеонаблюдения основаны на *клиент-серверной архитектуре*, и, как правило, вся обработка данных осуществляется на серверной стороне.

Ещё один подход состоит в вынесении части обработки данных на сторону клиента: в этом случае клиент связан с каждой камерой. В качестве примера можно привести задачу оцифровки видео в системах с аналоговыми видеокамерами. Можно осуществлять перевод в цифровой сигнал на стороне сервера и, соответственно, все камеры будут соединены с центральным постом коаксиальными кабелями, либо поставить *видеосервер* (*encoder*), который будет выполнять данную процедуру для нескольких камер и отправлять на сервер информацию в цифровом формате по IP.

Одним из основных недостатков традиционных систем видеонаблюдения является серьёзное снижение возможностей оперативного реагирования при росте масштабов системы. В случае, когда речь идет о нескольких десятках (и даже большем числе) входящих потоков видео, оператор уже не в состоянии адекватно отслеживать текущую обстановку в реальном времени. Согласно проведённым исследованиям, при большом числе контролируемых видеоканалов уже через 12 минут работы оператор пропускает до 45% активности на экране, а после 22 минут до 95%.

Эта проблема приобретает особенную актуальность при работе больших систем видеонаблюдения, скажем, если стоит задача отслеживать определённые объекты для всего города. Так, планомерное внедрение системы тотального видеонаблюдения в Лондоне (свыше 10000 камер в единой сети и более полумиллиона в целом по городу) не привело к серьёзному снижению количества инцидентов или повышению процента раскрытия преступлений.

Всё более востребованы системы видеонаблюдения, обеспечивающие построение решения с многоуровневой гибко

настраиваемой логикой, когда максимальное число процессов не требует постоянного активного участия оператора-человека. Подобные интеллектуальные системы позволяют решать не только задачи обеспечения безопасности, но могут быть полезны при решении бизнес-задач, сбора статистической информации об объектах наблюдения и т.д.

Получение точных данных о посещаемости наблюдаемого объекта, распределение посетителей по времени и даже возможность идентификации определённых групп клиентов (постоянных посетителей, интересующих демографических выборок) весьма актуальны для многих коммерческих организаций. В масштабе города это могут быть также задачи автоматического анализа загруженности транспортных потоков и ряд других сфер применения.

Современная система видеонаблюдения включает в себя множество различных технологий компьютерного зрения, как собственно технологии видеонаблюдения, так и технологии оптического распознавания символов (*optical character recognition; OCR*) или *биометрические технологии.*

Одними из важнейших функций видеонаблюдения являются *идентификация* и *классификация* людей. Для того, чтобы быть в состоянии идентифицировать человека по записанному видеоизображению его лица, необходимы знания о том, как в принципе выглядит этот человек. Это даст основание подтвердить, что идентифицировано именно это лицо.

Между тем, для классификации человека, не идентифицируя его, потребуется несколько меньше знаний; то есть, данная процедура является менее точной с точки зрения видеонаблюдения. Классификация означает визуальное определение пола, цвета одежды и других параметров. Поэтому для идентификации требуется бóльшая, чем для классификации, степень детализации изображения.

Комплексная технология интеллектуального видеонаблюдения должна включать следующие основные элементы и программно-алгоритмические модули:

- визуальные (ТВ, инфракрасные (ИК) и другие) датчики для дистанционного видеонаблюдения;
- средства распределённого сбора, сжатия, обработки и передачи цифровой видеоинформации по локальным и глобальным сетям в режиме реального времени;
- автоматическое выделение объектов наблюдения (люди, здания, транспортные средства и т.д.);
- автоматическое слежение за движущимися объектами в зоне наблюдения;
- биометрическое распознавание персонала, биометрический контроль доступа в критические зоны объекта наблюдения;
- автоматическую идентификацию транспортных средств, грузов и иных объектов посредством распознавания идентификационных меток (регистрационных номеров, штрих-кодов, других видов маркировки);
- методы оценки сценариев поведения наблюдаемых объектов и групп объектов;
- формирование тревожных сообщений оператору в случае возникновения неблагоприятных или нестандартных сценариев развития событий в зоне видеонаблюдения;
- программно-аппаратные средства для реализации методов и алгоритмов сбора и обработки видеоинформации.

Переход к цифровой обработке, передаче и хранению видеоинформации стал одним из важнейших направлений в индустрии видеонаблюдения. Иными словами, видеонаблю-дение ныне стало практически полностью цифровым. Сегодня почти все новые системы используют цифровые и IP-технологии для кодирования, передачи, просмотра и записи

видеосигнала. Видеонаблюдение настолько изменилось за последние годы, что можно вполне переименовать «видеонаблюдение» в «IP-наблюдение».

В свою очередь, наряду с ростом производительности и скорости микросхем памяти, процессоров и жёстких дисков отмечается постепенное уменьшение их стоимости. Поэтому цифровая обработка видеосигналов фактически стала единственным разумным методом обработки большого объёма качественных видеосигналов. В конечном счёте, ценность системы определяется не количеством фигурирующих в ней данных, а эффективностью их обработки.

В 2010 году на мировом рынке видеокамер (который оценивался примерно в $8 млрд) IP-камеры занимали лишь около 20%. Однако тенденция к переходу на IP-камеры уже сформировалась, и эти устройства начинают преобладать в отрасли.

Различие в подходе к построению клиент-серверных систем обработки видео проявляется и в том случае, когда речь идет о модулях *видеоаналитики*, призванных обеспечить автома-тизацию функций оператора системы видеонаблюдения. Принципиально возможны оба принципа размещения таких модулей – как на стороне сервера, так на стороне клиента. Тем не менее, по мере развития соответствующих технологий машинного зрения, обработка видео на стороне клиента получает всё большую поддержку у пользователей.

Отметим такое важное преимущество цифрового видео, как возможность проверки подлинности копии. Речь идёт о нанесении так называемых *«водяных знаков» (watermark)*. Это позволяет защитить информацию, записанную в цифровой форме, от подделки, что крайне важно для индустрии видеонаблюдения.

По прогнозам исследовательской компании *Research and Markets*, суммарные объёмы продаж на мировом рынке видеонаблюдения вырастут к 2022 году до $75 млрд.

В 2017-2022 годах мировой рынок видеонаблюдения будет расти в среднем на 15% ежегодно. Одним из важных стимулов такого роста станет продолжающийся переход с аналоговых на IP-камеры. Кроме того, важным фактором развития индустрии видеонаблюдения становятся «облачные технологии», открывающие качественно новые возможности для хранения и обеспечения доступа к собираемым данным. Также большое влияние оказывают галопирующие темпы роста спроса на услуги видеонаблюдения, как средство обеспечения безопасности.

Число объектов, оснащаемых системами видеонаблюдения, по-прежнему увеличивается во всём мире. Наиболее быстрый рост в предстоящие годы будет демонстрировать сегмент *«Видеонаблюдение как услуга» (Video Surveillance as a Service; VSaaS)*. Возрастает число приложений, которые успешно строятся на основе этого подхода, т. к., пользователи видят преимущества удалённого доступа к ресурсам видеосистем, хранящимся в «облачных» сервисах. Большое значение также имеет возможность подключаться к «живому» и записанному изображению не только со стационарных компьютеров, но и с мобильных устройств – благодаря чему видеонаблюдение может получить необходимый уровень удобства в пользовании и гибкости.

Если рассуждать об актуальности видеонаблюдения для финансовой сферы, то растущий спрос на подобные решения у банков и других организаций объясняется просто: за последние годы атаки на банкоматы стали настолько популярными, что в 2017 году на «чёрном рынке» впервые появилась услуга *ATM Malware-as-a-service*, когда злоумышленникам предоставляется готовое решение (программное обеспечение и набор оборудования) для взлома устройств самообслуживания. В т. н. *Darknet* можно купить все необходимые вредоносные программы и инструкции – и это не могло не отразиться на стремительном росте количества попыток взлома банкоматов во всём мире.

Защищать имущество, а также денежные средства и персональные данные клиентов банков, призваны специализированные системы видеонаблюдения. В качестве примера можно привести крупного североамериканского поставщика услуг для финансовых учреждений и розничных сетей, который планирует оснастить свой парк банкоматов в 9000 устройств, программным обеспечением *ATMeye.iQ.*

Развитие рынка видеонаблюдения и появление большого числа производителей определило спрос на открытые стандарты, обеспечивающие возможность совместного использования оборудования и программного обеспечения различных производителей. В настоящее время действуют уже два отраслевых объединения: *«Форум открытого сетевого видеоинтерфейса» (Open Network Video Interface Forum; ONVIF)* и *«Альянс за совместимость систем физической безопасности» (Physical Security Interoperability Alliance; PSIA)*. Обе организации были основаны в 2008 г. с целью создания стандартизированных интерфейсов для устройств физической безопасности и программных платформ, и совместимых систем обеспечения сохранности имущества, средств и чувствительных данных на базе IP-технологий.

Payments.iQ

Автоматизированная система управления платежами

Payments.iQ
.iQ Family Product

Payments.iQ – это программное решение для организации приема платежей (коммунальных услуг, налогов, штрафов), продажи любых видов электронных услуг (билетов, ваучеров и др.), автоматизации розничной банковской деятельности и управления сетями информационно-платежных терминалов самообслуживания и банкоматов.

Глава 1. Основные технологии видеонаблюдения

«Они могут следить за тобой день и ночь, но, если не потерял голову, ты можешь их перехитрить…»

Дж. Оруэлл, «1984»

Благодаря современным системам видеонаблюдения можно осуществлять визуальный контроль обстановки в помещениях и на прилегающих территориях. По способу получения и обработки изображений эти системы делятся на два типа: *аналоговые и цифровые.*

Системы аналогового видеонаблюдения, в основном, подходят для использования в небольших помещениях. Передача видеосигнала осуществляется по коаксиальному комбинированному кабелю, а подключение к системе регистрации (*видеорегистратору*) – при помощи BNC-разъёма.

Хотя аналоговые видеокамеры все ещё находят своё применение в современных системах видеонаблюдения, всё большее число производителей предлагают цифровые камеры для передачи видеопотока по компьютерным сетям. Ранее к тем немногим компонентам систем видеонаблюдения, работавшим с цифровым видео, относились устройства видеопамяти, видеоквадраторы, видеомультиплексоры, внутренние схемы камер с цифровой обработкой видеосигналов (*Digital Video Processing; DSP*).

Отметим, что в большинстве существующих систем видеонаблюдения, несмотря на использование аналоговых телекамер, имеются цифровые видеорегистраторы для наблюдения и долгосрочного хранения записей.

Помимо отображения оперативной обстановки и архивирования получаемой от видеокамер информации современными

средствами видеобезопасности могут быть обеспечены и другие функции, например, управление и наблюдение при помощи портативных устройств, оповещения посредством мобильной связи, *видеозахват* и распознавание автомобильных номеров, детектор оставленных вещей, а также идентификация личности по изображению лица человека.

Основной характеристикой качества системы видеонаблюдения является её техническая конфигурация. Существующие профессиональные системы видеонаблюдения состоят из разнообразных технических компонентов (камер, объективов, передатчиков сигнала, детекторов активности, инфракрасных подсветок, матричных видеокоммутаторов, тепловизоров, средств хранения изображений (*видеорегистраторов / видео-серверов*), компьютерных систем, мониторов и т.д.).

Разрешение видеокамеры всегда остаётся определяющим для оценки общего качества работы системы видеонаблюдения; тем не менее, крайне важно учитывать качество как записанного цифрового изображения, так и его обработки.

В последнее время предпочтение всё чаще отдаётся цифровым системам (IP) видеонаблюдения – несмотря на то, что их стоимость остаётся достаточно высокой. Тем не менее, цифровые системы видеонаблюдения во много раз превосходят стандартный мониторинг по своей функциональности.

IP-видеонаблюдение обеспечивает решение разносторонних практических задач при высоком качестве записи и масштабирования кадров. Несомненным его преимуществом является максимальная скорость обработки данных. Даже поворотная камера оперативного слежения способна фиксировать ряд случайных событий, чего нельзя сказать об аналоговом оборудовании.

По прогнозам аналитической компании IHS Markit, общее количество камер наблюдения в мире в 2018 г. должно составить 130 млн. Для сравнения, в 2006 г. их было менее 10 млн.

1.1. История появления и развития средств видеонаблюдения и видеоаналитики

Самые первые технические средства видеонаблюдения и видеоаналитики появились более 70 лет назад [1]. Процесс развития технологий видеонаблюдения можно разбить на три этапа.

Первый этап охватывает период 1942-1970 гг., когда впервые появились дорогостоящие, но довольно примитивные системы наблюдения, включавшие камеры и мониторы, соединенные между собой коаксиальным кабелем. При этом на каждую камеру приходился отдельный монитор. Качество изображений было крайне низким, менее 0,3 мегапикселя (Мп); к тому же, запись изображений на тот момент технически не была реализована.

В 70-е годы XX века для вывода на один монитор нескольких изображений появились *мультиплексоры*, а для записи изображений на магнитную плёнку – видеомагнитофоны. Эти устройства отличались низким качеством записи и не обладали технологической возможностью записи видео по событиям, или же функцией удалённого просмотра изображений.

На этом этапе в системах видеонаблюдения стали использоваться жёсткие магнитные диски, заменившие магнитные ленты. Благодаря им появились более массивные хранилища изображений с более высоким уровнем разрешения. Такие полуцифровые системы видеонаблюдения приобрели определённую технологическую гибкость, поскольку они уже обеспечивали удалённый доступ к изображениям по протоколу TCP\IP и архиву камер. Появилась возможность записи аудио сигнала, а в управлении камеры стали более удобными.

Наконец, третий этап ознаменовался появлением полностью цифровых систем видеонаблюдения, включающих в себя различные типы IP-камер с широким диапазоном возможностей,

универсальные кабельные инфраструктуры и программные комплексы видео регистрации. Эти системы обладают высокой интеграционной способностью; для организации систем видеонаблюдения отныне не требуется прокладка отдельных коаксиальных линий связи от камеры к серверу.

Цифровое видео проникло в индустрию вещательного телевидения в начале 1990-х годов – и стало в итоге новым стандартом, который пришёл на смену аналоговому ТВ.

В настоящее время имеются два наиболее распространенных варианта телевизионного вещания: *телевидение стандартной чёткости* (*Standard Definition; SDTV*)**,** которое характеризуется соотношением сторон 4:3 и обычным качеством – и *телевидение высокой чёткости (High Definition; HDTV*) с пятикратным увеличением качества передаваемого изображения. HDTV обычно предполагает широкое (16:9) соотношение сторон экрана и горизонтальное разрешение 1920 пикселей с прогрессивной развёрткой. Это создаёт разрешение кадра в 2 073 600 (1920x1080) пикселей. Частота кадров может меняться, и указывается после буквы p – например, 1080p30 или 1080p50.

Также имеются форматы HDTV, обозначаемые как 1080i и 720p. Хотя у них одинаковое (16:9) соотношение сторон, 1080i показывает 1920x1080 строк с чересстрочной развёрткой, в то время, как формат 720p отображает 1280x720 (921 600) пикселей с прогрессивным сканированием.

Телевизоры HDTV основаны на квадратных пикселах, аналогичных для экранов компьютеров, поэтому HDTV-видео от сетевых видео продуктов можно отображать на экранах HDTV или стандартных мониторах. Однако при использовании видео высокой чёткости с прогрессивной развёрткой не требуется применять метод преобразования или деинтерлейсинга, когда видео должно обрабатываться компьютером или отображаться на экране компьютера.

Во многих странах мира телевещание является цифровым – обычно, в обоих (SDTV и HDTV) форматах. Большинство же пользователей предпочитают стандарт HDTV (у которого разрешение и соотношение сторон выше, как у широкоформатного экрана кинотеатра) – однако в видеонаблюдении используется стандартное разрешение. Поэтому далее мы рассмотрим основные вопросы, связанные с цифровым видео стандартного разрешения с соотношением сторон 4:3.

Также стоит упомянуть разрешение *4K Ultra HD,* которое в 4 раза превышает стандартное разрешение *HDTV 1080p*. Для *4K Ultra HD* используется формат 16:9.

Разрешение *4K Ultra HD* ныне получает всё большее распространение на рынке, и переход на этот стандарт в системах видеонаблюдения гарантирует высокое качество видео с необходимой детализацией изображений.

Стандарт *4K Ultra HD* предусматривает использование квадратных пикселей, аналогичных имеющимся на экранах компьютеров, поэтому видео с разрешением *4K Ultra HD*, получаемое с устройств сетевого видеонаблюдения, может быть воспроизведено как на экранах HDTV, так и на стандартных компьютерных мониторах. Для видео *4K Ultra HD* с прогрессивной развёрткой не требуется применение каких бы то ни было методов деинтерлейсинга, если видео должно обрабатываться с помощью компьютера, или воспроизводиться на компьютерном экране.

1.2. Цифровое видеонаблюдение

У цифровых систем видеонаблюдения нет ограничений по возможностям передачи информации. В общих чертах цифровая передача имеет несколько важных отличий:

- информация передаётся в цифровом качестве;
- расширение матрицы обеспечивает получение изображения высокого разрешения (в формате *Full HD*);
- предусмотрены дистанционное управление и настройка;
- не требуется резервный источник питания.

Возможность дистанционной настройки является значительным преимуществом при запуске и монтаже системы. При этом всю систему цифрового видеонаблюдения можно настроить на базе уже налаженной офисной сети.

Современные системы видеонаблюдения состоят из сетевых камер (*network camera; NC*), видеосерверов (*video server; VS*), сетевых видеорегистраторов (*network video register*) и сетевых видеорегистраторов на основе программного обеспечения (*software network video register; SNVR*) [1].

Современные камеры делятся на *проводные* и *беспроводные*. По типу устройства входа их также разделяют на *аналоговые* и *цифровые*.

Аналоговая система устроена по принципу передачи сигнала с источника без искажения его плавности. Цифровая аппаратура передаёт видеосигнал, предварительно разделив его на части, и затем собрав его уже в двоичной системе. Цифровую запись в отличие от аналоговой можно воспроизвести на компьютере. Данное обстоятельство является важным свойством цифрового видеонаблюдения.

По характеру цветности оборудование разделяется на *чёрно-белую*, *цветную* и *с инфракрасной подсветкой.*

Чёрно-белое цифровое телевещание отличается особой чувствительностью и может быть использовано даже при недостаточном освещении – или даже его отсутствии. Такая

аппаратура хорошо фокусирует мельчайшие детали при удалённости объекта наблюдения.

Работая с прогрессивной развёрткой, сетевые камеры с производительностью HDTV обеспечивают истинное представление о цвете и чёткие изображения, даже если объект движется быстро. Это весьма востребованное решение для операций контроля, когда требуется более подробная информация о деталях – например, в аэропортах, на паспортном контроле, в казино или на автомагистралях. Такое качество не могло быть достигнуто до тех пор, пока методы сжатия видео не стали достаточно эффективными.

Стоит отметить профессиональные сетевые камеры с объективом *Fisheye* с ультрашироким обзором и с богатыми функциями, которые имеют высокое качество изображений, необходимое для многих приложений.

Термин *«битрейт»* (англ. *bitrate*) используется для определения ширины видеопотока при измерении эффективной скорости передачи потока данных по каналу, т.е., минимального размера канала, который сможет пропустить этот поток без задержек – и обозначает количество бит, используемых для передачи / обработки данных за единицу времени. Выражается битами в секунду (*бит/с, bps*), а также производными величинами с приставками «кило-» (*кбит/с, kbps*), «мега-» (*Мбит/с, Mbps*) и т. д. (например, для стандарта DVD-видео ширина потока составляет около 5 Мбит/с – а для формата ТВ высокой чёткости (*HDTV*) – уже 10 Мбит/с). Чем выше «битрейт», тем выше качество. Зачастую «битрейт» используется для оценки качества видео, транслируемого через Интернет.

1.2.1. Популярные форматы изображений, используемые в цифровом видеонаблюдении

Созданная в 1988 году экспертная группа по вопросам кинотехники *Moving Picture Experts Group (MPEG)* разработала стандарты кодирования аудио и видео для различных прикладных областей – таких, как хранение, распространение и передача цифровой информации.

Хотя в видеонаблюдении обычно используется видеосигнал, и речь идёт о сжатии движущихся изображений, нашло применение и сжатие отдельных неподвижных изображений. Для различения этих видов сжатия часто говорят о сжатии *подвижного* и *неподвижного* видеоизображения.

Отметим, что для размещения минутного несжатого видео с частотой 30 кадров в секунду разрешением 720x576 пикселей и 16-битной глубиной цвета потребуется около 1,5 Гб свободного дискового пространства (это без учёта звуковой дорожки).

Поэтому исходный цифровой видеосигнал, как правило, подвергается определённому преобразованию для сжатия в соответствии и принятыми стандартами.

JPEG (Joint Photographic Experts Group – англ. *Объединённая группа экспертов по машинной обработке фотографических изображений***,*** по названию организации-разработчика) — один из популярных графических форматов, применяемый для хранения фото и иных изображений. Файлы в формате JPEG обычно имеют расширения .jpeg, .jfif, .jpg, .JPG или .JPE. .jpg является наиболее популярным на всех платформах.

Алгоритм *JPEG* позволяет сжимать изображение как *с потерями*, так и *без потерь* (режим сжатия *lossless JPEG*).

Поддерживаются изображения с линейным размером не более 65535 × 65535 пикселей.

К недостаткам сжатия по стандарту JPEG следует отнести появление на восстановленных изображениях при высоких степенях сжатия характерных артефактов – изображение рассыпается на блоки размером 8x8 пикселей (этот эффект особенно заметен на областях изображения с плавными изменениями яркости), в областях с высокой пространственной частотой (например, на контрастных контурах и границах изображения) возникают артефакты в виде шумовых ореолов. Следует отметить, что стандарт JPEG (ISO/IEC 10918-1, Annex K, п. K.8) предусматривает использование специальных фильтров для подавления блоковых артефактов, однако на практике подобные фильтры, несмотря на их высокую эффективность, практически не используются. Невзирая на недостатки, JPEG получил широкое распространение благодаря достаточно высокой (относительно существовавших во время его появления альтернатив) степени сжатия, поддержке сжатия полноцветных изображений и относительно невысокой вычислительной сложности.

Motion JPEG или M-JPEG — цифровой видеоряд, состоящий из последовательности отдельных статичных изображений JPEG. Отметим, что отображение 16 или более кадров в секунду воспринимается зрителем как видеоизображение. Отображение 30 (NTSC) или 25 (PAL) кадров в секунду воспринимается как полноценное видео. Одно из преимуществ *Motion JPEG* состоит в том, что каждому кадру гарантируется качество, получаемое на уровне сжатия, выбранном для сетевой камеры или видео кодера. Чем выше уровень сжатия, тем меньше размер файла и ниже качество изображения. В некоторых случаях, например, при слабом освещении или более сложном объекте наблюдения, размер файла изображения может только увеличиться, поэтому для его хранения и передачи потребуются более высокая

пропускная способность и больший объём памяти.

Сетевые видеоустройства некоторых производителей позволяют выбирать максимальный размер изображения кадра для предотвращения роста пропускной способности и объёма памяти. Отсутствие взаимосвязи между кадрами в *Motion JPEG* гарантирует высокую надёжность этого формата, т.е., потеря одного кадра во время передачи не повлияет на качество остального видеоряда.

Motion JPEG — не лицензируемый стандарт сжатия. Благодаря своей совместимости, этот формат широко используется в приложениях, требующих наличия отдельных кадров в видеоряде (например, для анализа) и использующих меньшую (обычно 5 кадров в секунду) частоту кадров. *Motion JPEG* также может использоваться в приложениях, требующих интеграции с системами, поддерживающими только формат *Motion JPEG*. В результате, по сравнению с такими стандартами, как *MPEG-4* и *H.264*, файлы в формате *Motion JPEG* характеризуются более высокой скоростью передачи данных или низким уровнем сжатия.

Стандарты сжатия. В настоящее время существует множество популярных форматов сжатия на основе различных алгоритмов компрессии:

DV (Digital Video) – один из первых алгоритмов сжатия для видеопотока, разработка которого началась в 1993 году совместно крупнейшими производителями видеооборудования (*Sony, JVC, Panasonic, Philips* и *Hitachi*). Формат *DV* обеспечивает степень сжатия данных (5:1) и характеризуется высоким битрейтом, что приводит к большому размеру выходного видеофайла. К примеру, 1-минутный DV-видеоролик занимает на цифровых носителях информации около 200 Мб (1 час – 12 Гб).

Чаще всего этот формат используется для сжатия при видеосъёмке с помощью бытовых цифровых камер и профессиональных камкордеров. При этом благодаря небольшому коэффициенту сжатия отснятые материалы имеют весьма высокое качество, а сама процедура сжатия выполняется в реальном времени, не требуя мощных технических компонентов.

MPEG – целое семейство стандартов сжатия цифровой информации, разработанное и стандартизированное одноимённой экспертной группой. Первым из них стал исходный стандарт видео и аудио компрессии *MPEG-1*, а в 1993 году при участии компаний *JVC* и *Philips* была разработана его спецификация *Video CD (VCD)*, которая известна многим пользователям. Этот стандарт является форматом для хранения сжатого видео и аудио на обычных компакт-дисках.

Применение для кодирования алгоритмов MPEG-1 позволяет получать видеопоток шириной до 1,5 Мбит/с с разрешением кадра 352x288 точек для *PAL* или 352x240 для *NTSC*. В 1995 году был предложен стандарт *MPEG-2*, получивший широкое распространение в цифровых видеодисках *(DVD)*, а также при передаче сигнала кабельного и спутникового ТВ. При этом качество картинки здесь значительно выше, чем у предшественника: при 25 кадрах в секунду разрешение составляет 720x576 точек для системы *PAL*, а для системы *NTSC* – 720x480 при 30 кадрах/с. При этом средняя максимальная ширина потока равна 9,8 Мбит/с, что практически в 7 раз выше, чем у *Video CD*. Ещё одним неоспоримым преимуществом *MPEG-2* является возможность сохранения пятиканальной аудиодорожки (*Dolby Digital 5.1* и *DTS*).

Наряду с *MPEG-2* велась разработка ещё одного стандарта, *MPEG-3*, предназначенного для кодирования аудио- и видеопотоков в телевидении высокой чёткости со скоростью передачи данных от 20 до 40 Мбит/с. Тем не менее, оказалось,

что с этой целью можно использовать модифицированную версию стандарта *MPEG-2* – что привело к прекращению дальнейших разработок по *MPEG-3*. Ныне этот стандарт более не используется.

Наконец, в 1998 году появилось новое семейство форматов сжатия видео – *MPEG-4,* предназначенное для улучшения качества картинки при низкой скорости потока. Прежний стандарт *MPEG-2*, рассчитанный на высокий битрейт, с этой задачей справиться не мог – поэтому алгоритмы сжатия были существенно модифицированы. Также *MPEG-2* не подходит и для хранения видео высокой чёткости (*HD*) с разрешениями от 1280x720 (720p) до 1920x1080 пикселей (1080i или 1080p), которое становится всё более популярным.

Как правило, в системах видеонаблюдения формат *MPEG-4* соответствует стандарту *MPEG-4 Part 2*, известному также как *MPEG-4 Visual*. Подобно всем стандартам *MPEG*, этот стандарт является лицензированным, поэтому пользователи должны приобретать лицензию на каждую станцию мониторинга. Формат *MPEG-4* используется в приложениях с невысокой пропускной способностью, а также в приложениях, требующих высокого качества изображения, фактически неограниченную пропускную способность и отсутствие ограничений по частоте кадров.

Ныне *MPEG-4* является основным стандартом сжатия мультимедиа контента, и, хотя списывать со счетов *DVD* ещё рано, практически все современные фото- и видеокамеры снимают в HD-качестве.

Кодеки. Поскольку для сжатия видео могут использоваться различные стандарты, при выборе определённого алгоритма преобразования данных можно сжать видео различными инструментами или программными средствами, что даёт на выходе совершенно различные результаты.

Во многом все эти отличия как раз и определяются *кодеком* – специальной программой, осуществляющей сжатие (кодирование) исходных материалов. При этом каждый из них использует свой собственный алгоритм, который влияет как на качество, так и на скорость кодирования.

Термин «кодек» является сокращением от двух слов «**ко**дер» и «**дек**одер». Это значит, что кодек должен включать в себя не только модуль сжатия (кодер), но и модуль просмотра (декодер). Последние обычно распространяются бесплатно, и входят в популярные наборы кодеков, таких как *K-Lite Codec Pack* или *Windows 7 Codec Pack*.

Рассмотрим несколько наиболее распространенных видов кодеков.

MPEG-4 Part 2 ASP - один из первых алгоритмов, предложенный в 1999 году. Построенные на его основе кодеки обеспечивают довольно низкое качество. Тем не менее, этот недостаток частично компенсируется высокой скоростью работы и низкими требованиями к аппаратным ресурсам. Известные кодеки, основанные на этих алгоритмах – это коммерческий *DivX* и его бесплатная альтернатива *XviD*.

MPEG-4 AVC10/AVS или *H.264* – один из популярных алгоритмов, используемый как для сжатия видео с низким разрешением, так для и HD контента. Аббревиатура *AVC* расшифровывается как *advanced video coding* («передовое кодирование видеосигналов»). Как и в предыдущем случае, у этого семейства кодеков существуют как бесплатные (например, *x.264*), так и коммерческие варианты, входящие в состав популярных видео редакторов.

H.264 является открытым лицензионным стандартом, способным уменьшить размер цифрового видеофайла без ущерба для качества изображения. Можно утверждать, что *H.264* стал необходимой предпосылкой для внедрения *HDTV* в

видеонаблюдение. Эффективное сжатие одновременно обеспечивает высокое разрешение, высокую частоту кадров и соотношение сторон 16:9.

Ожидается, что в ближайшие годы стандарт *H.264* станет одним из наиболее востребованных. Кодер *H.264* без ущерба для качества изображения может уменьшать размер файла цифрового видео более чем на 80% по сравнению с форматом *Motion JPEG* и на 50% — по сравнению со стандартом *MPEG-4*. Это, с одной стороны, означает менее жёсткие требования к полосе пропускания для передачи и объёму памяти для хранения видеофайла, а с другой – даёт возможность получать видеоизображения более высокого качества при той же скорости передачи данных.

В отрасли охранного видеонаблюдения *H.264*, по всей вероятности, найдёт своё применение в областях, требующих использования высокой частоты кадров и высокого разрешения – например, для охранного наблюдения за автомагистралями, аэропортами и казино, где нормой является использование частоты 30/25 (*NTSC/PAL*) кадров в секунду. Наибольшая экономия будет достигнута за счёт снижения требований к ширине полосы пропускания и объёму свободного пространства для хранения данных.

Медиаконтейнеры и их форматы. Цифровая информация, видео хранится в виде файлов, или как их ещё называют, медиаконтейнеров, содержащих видео-, аудио- и другие потоки, а также метаданные. В любой момент из такого контейнера можно извлечь, например, видео или аудиодорожки, перекодировать их, поместить их в другой контейнер, т.е., изменить формат видеофайла. Мультимедийные контейнеры могут быть разных типов (форматов).

Несмотря на то, что большинство контейнеров привязаны к определённому формату, некоторые из них могут хранить видео в различных стандартах. Например, файл с расширением *AVI*

способен содержать ролики в форматах *MPEG-1*, *MPEG-2* или *MPEG-4*. Заметное влияние на качество видео оказывает выбор кодека, а также установленных при сжатии параметров. Однако и от контейнера зависит немало. Различные виды видеофайлов имеют определённые требования и ограничения по количеству звуковых дорожек, каналов субтитров, типов используемых кодеков, совместимости с бытовыми проигрывателями и плеерами и т.д.

Медиаконтейнер *AVI (Audio Video Interleave)*, впервые использованный компанией *Microsoft* в 1992 году, может содержать сжатую различными комбинациями кодеков видео- и аудиоинформацию. Таким образом, при внешнем сходстве *AVI*-файлы могут существенно различаться внутренней «начинкой».

Строго говоря, контейнер *AVI* давно устарел – и имеет ряд серьёзных недостатков: невозможность содержания смешанного видео (например, *NTSC* и *PAL*) и альтернативных аудиодорожек, отсутствие меток времени и индексов кадра, невозможность нормальной работы с субтитрами и т.д. Тем не менее, огромное количество медиа контента в Интернете и по сей день распространяется именно с помощью этого формата – благодаря, скорее всего, его универсальности.

MP4 (MPEG-4 Part 14) – один из современных форматов файлов для хранения цифровых видео- и аудио- потоков, являющийся частью стандарта *MPEG-4*.

TS и *M2TS*– специализированные контейнеры для хранения *HD*-видео. *TS* используется в потоковом вещании цифрового ТВ *IPTV* и *DVB*. *M2TS* является стандартным контейнером для *Blu-Ray* видео, в который могут быть включены видео- и аудио-потоки, предусмотренные стандартом *BD-ROM*, а также субтитры в графическом формате *PGS*.

1.2.2. Цифровые видеорегистраторы

Цифровые видеорегистраторы (*digital video recorder; DVR*) предназначены для многофункциональной работы с видеоизображением (включая приём, обработку, передачу и запись видеоинформации).

Видеорегистраторы используются в построении систем видеонаблюдения:
для наблюдения за определёнными участками, например, за торговыми залами, офисными помещениями с целью предупреждения незаконного проникновения; также их устанавливают на рабочих местах в банках, на автомобильных стоянках, автозаправочных станциях, охранных дорожных постах, транспортных предприятиях с целью фиксации действий посетителей и сотрудников и т.д.

Перечислим основные типы видеорегистраторов:

- *Цифровые видеорегистраторы (DVR)* используются для присоединения аналоговых видеокамер. Эти видеокамеры подключаются к цифровому *DVR* с помощью кабеля через разъём *BNC*. *DVR* принимает с камер несжатый видеопоток, сжимает и сохраняет его. Преимуществами *DVR* являются независимость обработки сигнала (он обрабатывается и архивируется на регистраторе) и полноценное функционирование вне зависимости от условий подключения к Интернету.
- *Сетевые видеорегистраторы (network video recorder; NVR)* подключаются к *IP*-видеокамерам и используют для создания сгруппированной в разных местах системы наблюдения, которая управляется центральным пунктом контроля. *NVR* принимает сигнал в сжатом виде. Преимуществами системы являются гибкость программного обеспечения и качественное изображение, получаемое с *IP*-камер.

- *Регистраторы-гибриды (hybrid video recorder)* — это промежуточный вид записывающих устройств, приспособленных для получения сигнала с аналоговых и *IP*-камер. Аналоговые видеокамеры подсоединяются к регистратору гибриду через порт *BNC*, а Интернет-протокольные (*IP*) — через Интернет. Регистраторы гибриды сочетают преимущества цифровых видеорегистраторов *DVR* и *NVR*. С их помощью устанавливаются гибкие в применении системы видеонаблюдения, способные обрабатывать потоки двух видов. Такие видеорегистраторы записывают информацию в локальных и сетевых архивах.

К числу базовых параметров при выборе видеорегистратора следует отметить наличие мультиканальности. Выпускаются регистраторы ёмкостью от 4 до 32 каналов.

Цифровые видеорегистраторы и сетевые телекамеры способствовали как развитию отрасли, так и разработке «интеллектуальных» систем видеонаблюдения. Благодаря им практически стирается граница между компьютерами, сетевыми и информационными технологиями, и видеонаблюдением.

1.2.3. Видеосерверы

Видеосервер (*video server; VS*) — компьютерное устройство (сервер), предназначенное для приёма, хранения, воспроизведения или ретрансляции видео- и/или аудиосигнала; обработки изображений, в т. ч., полученных в инфракрасном спектре; при обработке данных телеметрии; управлении другими системами безопасности. По функциональности видеосервер является определённой точкой в эволюции цифрового видеомагнитофона.

Видеосерверы широко применяются в системах видеонаблюдения и аудиоконтроля в качестве промежуточного оборудования. Они могут использоваться и как конечные устройства (если они установлены непосредственно в помещениях, используемых для контроля видео- и аудиоинформации). Существуют как готовые серийные видеосерверы, так и платы видео- и аудиозахвата со специальным программным обеспечением, с помощью которых можно самостоятельно собрать видеосервер.

Кроме того, видеосерверы могут быть ядром интегрированных систем безопасности. В таких системах они могут: управлять системой контроля доступа (используется программно-аппаратная обработка изображений с распознаванием лиц, номеров автомобилей, в вагонов и др.); осуществлять обработку аудио сигналов с распознаванием голоса; применять тепловизоры (например, для определения уровня жидкости в цистерне или равномерности прогрева объектов наблюдения); использовать радары для определения скорости движения транспортных средств и т.д.

В интегрированных системах безопасности видеосерверы зачастую используются и как управляющие устройства для систем оповещения, охранной и пожарной сигнализации. Кроме того, на современном этапе развития видеосерверы используются для обработки различных элементов телеметрии, контроля кассовых операций в банках и для учёта рабочего времени на предприятиях.

1.3. Сетевые технологии в видеонаблюдении

В решениях для охранного видеонаблюдения качество изображения является определяющим в целях четкой фиксации происходящего и идентификации участников в зоне контроля.

Благодаря использованию прогрессивной развёртки и мегапиксельной технологии в сетевых камерах можно достичь лучшего качества и большего разрешения изображения, чем в аналоговых камерах.

Также следует отметить, что добиться высокого качества изображения в системе сетевого видеонаблюдения значительно проще, чем в аналоговых системах охранного наблюдения. В настоящее время в аналоговых системах, использующих цифровые видеорегистраторы, выполняются несколько аналого-цифровых преобразований – вначале аналоговые сигналы преобразуются в камере в цифровые, затем обратно в аналоговые для передачи, и, наконец, вновь оцифровываются при записи. При этом качество сохраняемого изображения с каждым новым преобразованием и при большой протяженности кабелей ухудшается. Кроме того, чем больше дальность передачи аналогового видеосигнала, тем слабее он становится.

1.3.1. IP-камеры

Как и в любой системе видеонаблюдения основой цифрового видеоконтроля являются камеры. *IP-камера* представляет собой цифровую видеокамеру, предназначенную для передачи видеопотока в цифровом формате по сетям *Ethernet* и *TokenRing*, использующим протокол *IP*. При этом как сетевое устройство, так и каждая *IP-камера* в сети имеет свой *IP-адрес*.

В отличие от аналоговых камер, при использовании IP-камер после получения видеокадра с прибора с зарядовой связью (*ПЗС*; англ. *charge-coupled device; CCD*) или светочувствительной матрицы камеры на основе КМОП-технологии (англ. *complementary metal-oxide semiconductor*; *CMOS*) изображение остаётся цифровым вплоть до отображения

на мониторе. Просмотр этого изображения возможен с помощью браузера, установленного на компьютере – а для просмотра, обработки, записи изображения с сетевых камер имеется ряд программно-аппаратных средств.

Работая с прогрессивной развёрткой, сетевые камеры с производительностью *HDTV* обеспечивают истинное представление о цвете и чёткие изображения, даже если объект движется быстро. Поэтому такие камеры обладают явным преимуществом для операций контроля, где требуется более подробная информация о деталях – например, в аэропортах и на автомагистралях.

Использование IP-систем также называют цифровым или сетевым видеонаблюдением, поскольку оно построено по принципу компьютерной сети, обладает всеми присущими ей возможностями, достоинствами и недостатками (естественно, с учётом задач, которые возлагаются на систему видеонаблюдения как средство обеспечения безопасности).

1.3.2. IP-видеонаблюдение

Базовыми компонентами *системы сетевого видеонаблюдения (*или *охранного IP-видеонаблюдения*) являются сетевая камера, видеокодер (применяется для подключения аналоговых камер), сеть, сервер и система хранения, а также программное обеспечение для управления видео.

В качестве среды передачи видео, аудио и других данных системы сетевого видеонаблюдения используют проводную или беспроводную IP-сеть. При использовании технологии *Power over Ethernet* (*PoE*) по сети также можно осуществлять питание устройств сетевого видеонаблюдения. Отметим, что для аналоговых систем эта технология недоступна.

Разработанные на основе компьютеров сетевые камеры и видеокодеры располагают возможностями, которые недоступны для аналоговых камер. В полностью цифровой системе IP-видеонаблюдения изображение оцифровывается один раз в сетевой камере – и затем остаётся в цифровом формате без лишних преобразований, потерь качества и зависимости от дальности передачи по сети. Кроме того, цифровое изображение проще хранить по сравнению с аналоговыми видеокассетами.

Система сетевого видеонаблюдения позволяет просматривать и записывать видео из любой точки сети, вне зависимости от того, локальная это сеть, или же глобальная. IP-видеонаблюдение легко масштабируется – что, безусловно, является её достоинством.

Сеть, системы хранения и серверы в целом составляют стандартное ИТ-оборудование для системы сетевого видеонаблюдения. Совокупная стоимость владения системой IP-видеонаблюдения обычно ниже, чем традиционной аналоговой.

Зачастую в организации уже имеется сетевая IP-инфраструктура, которую можно использовать для сетевой системы видеонаблюдения. Проводные и беспроводные IP-сети в целом являются менее дорогой альтернативой традиционным коаксиальным и оптическим кабельным сетям для аналоговых систем видеонаблюдения. Кроме того, цифровые видеопотоки могут передаваться по всему миру по различным каналам связи. Применение серверного оборудования, соответствующего промышленным, и открытым стандартам для записи и хранения (а не закрытого специализированного аппаратного обеспечения – как в случае с цифровыми видеорегистраторами в аналоговых системах видеонаблюдения) также позволяет снизить затраты на оборудование и управление всей системой.

По количеству пользователей сетевые системы видеонаблюдения практически не имеют ограничений. Однако в

большинстве случаев доступ лимитируется из-за опасности несанкционированного доступа.

IP-камеры подключаются в существующую локальную сеть организации и любой вычислительной станции. Как правило, производители IP-камер в комплекте поставляют программу для видеорегистрации.

К преимуществам системы IP-видеонаблюдения можно отнести такие факторы:

- оборудование быстро подключается и настраивается;
- IP-камера позволяет передавать видеосигнал высокого качества в цифровом режиме;
- IP-видеонаблюдение может быть внедрено на базе уже действующих видеокамер и сетевого оборудования;
- для мобильного применения достаточно подключить его к смартфону, планшету или ноутбуку.

IP-камера оснащается интерфейсом *Wi-Fi* или *Ethernet* и подключается к локальной сети. В такую камеру встраивается веб-сервер, поэтому изображения можно просматривать из любой точки мира. Благодаря шифрованию сигнала при использовании устройства повышается защищённость передаваемой информации. При этом каждая IP-камера оснащена функцией записи в случае фиксации движения; кроме того, минимизируется риск несанкционированного подключения к системе.

Хотя большое разрешение камер приводит к увеличению передаваемого потока данных, создавая дополнительную нагрузку на сеть, для решения многих задач вполне достаточно порядка 100 пикселей на 1 метр зоны наблюдения. Более того, многие мегапиксельные видеокамеры попросту не способны обеспечить передачу изображения с частотой больше 10-15 кадров/сек.

С учётом сказанного, после оптимизации разрешающей способности IP-камер нужно выбрать подходящий тип сжатия – скажем, *H.264* или *MPEG*.

1.3.3. Удалённое управление системами видеонаблюдения (VSaaS)

Видеонаблюдение как сервис (*video surveillance as a service*; *VSaaS*) на базе «облачной» инфраструктуры — это важное направление для развития отрасли. По данным агентства *IMS Research* (Великобритания), глобальный рынок *VSaaS* составил $500 млн в 2011 году и за последующие 3 года удвоился. Данные по США свидетельствуют, что рынок инструментов видеоаналитики для бизнеса вырос с 2011 по 2016 год более чем в 2,5 раза и составил $900 млн.

В отличие от классической системы управления видео пользовательский интерфейс «облачного» приложения для предоставления услуги *VSaaS* должен быть реализован на базе браузера или мобильного телефона. При этом *VSaaS* предполагает использование более сложных технологий для управления каналом связи между объектом наблюдения и «облаком», а также между «облаком» и абонентом. Если система управления видео предполагает наличие постоянных операторов перед мониторами охранного телевидения, абоненты *VSaaS* чаще всего подключаются к системе через браузер лишь после поступления тревожного сообщения, или для анализа видеоархива (отчётов) [11].

Для внедрения *VSaaS* заказчик вместо того, чтобы развёртывать у себя полномасштабную инфраструктуру для сбора, хранения и обработки видеоданных, устанавливает видеокамеры в требуемых местах – а большую часть оставшихся функций

возлагает на провайдера. В зависимости от разграничения «зон ответственности» между заказчиком и поставщиком услуги *VSaaS* делятся на *видеохостинг* (видео с камер сразу передаётся в центр обработки (и хранения) данных (*data center; ЦОД*) провайдера, и сервис управления видеонаблюдением (когда видео хранится у заказчика, а провайдер осуществляет лишь удалённое управление). Кроме того, возможны комбинированные варианты – например, сохранение копии видео у заказчика с целью резервирования.

Преимущества модели *VSaaS* многочисленны. Пользователям больше не надо покупать дорогостоящее цифровое (*DVR*) или сетевое (*NVR*) оборудование, а также брать на себя обязанность по обеспечению его исправности, сохранности и защиты от различных атак. Кроме того, отпадает необходимость в приобретении лицензий на программное обеспечение для управления видео (*Video Management System; VMS*), т.к. доступ к видеопотокам с камер и средствам для его анализа предоставляется через Интернет.

Очевидные преимущества модели *VSaaS* привели к тому, что облачные услуги видеонаблюдения стали предлагать множество компаний во всём мире, среди которых – традиционные поставщики видеокамер и приложений *VMS*; фирмы, специализирующиеся на средствах контроля доступа и системах видеоаналитики, а также многочисленные стартапы. По оценкам *IMS Research*, объём мирового рынка услуг *VSaaS* в ближайшие три года должна удвоиться. Основанием для такого прогноза служит разнообразие сфер применения услуг *VSaaS*.

Многие компании предлагают лишь базовые функции управления видео, взымая дополнительную плату за расширенную функциональность подобных решений. Пока лишь единичные поставщики реализовали функции видеоаналитики (*Archerfish*, *VIAAS*) или интеграцию со средствами контроля доступа (*Brivo*). Всё больше провайдеров

предлагают поддержку локальных устройств хранения на стороне клиента (камер с SD-картами, либо камер, подключаемых к *DVR* или системам *NAS*); тем не менее, подобная функциональность ещё не стала повсеместной. Как правило, ежемесячная плата за услуги *VSaaS* составляет $5-30 за камеру.

«Видеонаблюдение как сервис» фокусируется на видеоанализе без участия оператора – в то время, как термин *VSaaS* сегодня чаще предполагает лишь возможность удалённого просмотра и записи без какой-либо аналитики.

Для определённых сегментов пользователей услуга *VSaaS* более предпочтительна, нежели классические решения на базе сетевых видеорегистраторов и систем управления видео. Так, модель коммерциализации *VSaaS* предполагает, что вместо стоимости аппаратно-программного решения без гарантий возврата инвестиций потребитель оплачивает конкретную услугу, например, запись видео, автоматический вызов службы охраны, сбор данных и подготовку аналитических отчётов. Услуга *VSaaS* является масштабируемой по объёму хранимого видео, количества точек наблюдения и числа пользователей системы.

Видеоаналитику можно рассматривать как специализированный кодер, который оставляет лишь нужные пользователю данные. Универсальный кодер, такой, как *H.264*, «не понимает» степени важности каждого элемента на изображении – и поэтому он не способен эффективно фильтровать избыточные данные для предоставления услуги *VSaaS*. Например, стандартный кодер не в состоянии отличить фигуру человека на заднем, и снежинку – на переднем плане. Если человек и каждая снежинка кодируются с одинаковой детализацией, видеопоток будет избыточен для передачи и хранения.

Видеоаналитика представляется единственной технологией, способной разрешить проблемы исходящего канала абонента, а также хранения видео в облаке. Несмотря на появление экономичных способов хранения видео, таких, как *LAID* (*LinearArrayofIdleDisks*), хранение больших объёмов видео в «облаке» является наиболее затратной составляющей услуги *VSaaS.*

В настоящее время в мире наблюдается сдвиг от локальной биометрии к облачной; облачная биометрия в своём развитии опережает локальную, в первую очередь, в финансовых приложениях [10]. Об этом свидетельствуют результаты исследования, проведённого компанией *Acuity Market Intelligence.*

Такое изменение не означает, что локальная биометрия, которая основана на оборудовании, установленном непосредственно на объекте, становится менее важной. Специалисты компании предсказывают, что к 2022 году в мире будет использоваться 5,6 млрд мобильных биометрических устройств, выполняющих за год 1,4 трлн транзакций.

Если в локальной биометрии пользователь связывается лишь с определённым устройством, то в облачной биометрии выполняется проверка его уникальной проверяемой идентичности, не зависящая ни от устройства, ни от платформы, на которой оно работает.

Кроме того, облачная биометрия может дополняться и усиливаться поведенческой биометрией, что обеспечит постоянную пассивную аутентификацию людей, попадающих в сферу её действия.

1.4. Обзор состояния рынка средств по видеобезопасности

В настоящее время на рынке видеонаблюдения можно выделить следующие сегменты:

- сетевые камеры;
- сетевые видеорегистраторы, в том числе, на основе программного обеспечения;
- видеосерверы.

Видеонаблюдение становится основой для всё большего количества проектов. По оценкам компании *IMS Research* ежегодный прирост мирового рынка видеонаблюдения составляет 12%.

Широкая распространённость IP-камер, постоянное снижение их цен и расширение функционала положительно влияют на динамику развития этого рынка. Такое же воздействие оказывают на рынок и облачные технологии, позволяющие сокращать затраты заказчиков на оборудование. При этом сам переход на облако подталкивается необходимостью обрабатывать всё возрастающие объёмы данных, для чего используются технологические принципы *Big Data*.

В сегменте сетевых камер наблюдается неуклонный прогресс, появляются более функциональные решения видеоаналитики – а в решениях управления системами видеонаблюдения (*VMS*) и физической безопасности предлагаются дружественные пользовательские интерфейсы.

В 2017 году во всём мире через профессиональные каналы продаж были отправлены 98 млн сетевых камер и 29 млн камер видеонаблюдения *HD CCTV*. Кроме того, правоохранительным органам различных стран мира было поставлено 400 тыс. нательных камер. [9].

Спрос на некоторые типы камер– включая панорамные (с обзором 180 и 360 градусов), стереоскопические и термокамеры – будет расти особенно быстро.

Компания *Arecont Vision* планирует в полной мере воспользоваться ростом спроса на панорамное видеонаблюдение, используя мегапиксельные камеры с широким динамическим диапазоном. Комбинируя в одном кадре участки сцены, экспонируемые с бóльшими и меньшими значениями выдержки, технология расширения динамического диапазона *WDR* позволяет довести до максимума количество ценных деталей в ярких и затемнённых частях сцены.

Развитие видеоаналитики и «Интернета вещей» (*Internet of Things; IoT*) также способствуют росту спроса на видеонаблюдение. Видеоаналитика позволяет автоматически обрабатывать изображение вместо его просмотра человеком, а «Интернет вещей» делает видеонаблюдение частью «умного дома» (или же «умного офиса») – что также повышает спрос на решение [7].

В ряде стран заметна роль видеонаблюдения в снижении преступности. В частности, к 2020 году в Китае планируется взять под наблюдение все ключевые общественные места в стране. В Германии принят закон, который поощряет видеонаблюдение на стадионах, вокзалах и в магазинах, а также разрешает полицейским носить нательные камеры.

Сегменты рынка, где есть серьёзные заказчики на услуги видеонаблюдения, включают транспорт, банковский сектор, коммунальные сети и поставку энергоносителей – тем не менее, и в этих сегментах требования заказчиков к системам видеонаблюдения стремительно меняются.

Ныне организации желают использовать технологии видеонаблюдения в большей степени, нежели традиционное ведение видеозаписи и мониторинг безопасности (*security monitoring*) в режиме реального времени. Существенно изменился подход заказчиков к обеспечению безопасности

таких крупных протяжённых объектов, как автостоянки, склады, стадионы, конференц-залы, фитнес-центры и спортивные арены. Для решения такой задачи в масштабах стадиона может потребоваться до 2000 телекамер и многие сотни километров кабеля. Между тем, современные технологии позволяют полностью «накрыть» стадион при помощи всего 75 камер.

Преимущества IP-систем для решения вопросов безопасности банков оказались не столь очевидными. Учитывая тот факт, что банки успели основательно вложиться в инфраструктуру аналогового *CCTV*, ни о какой миграции к сетевым системам у многих заказчиков в этом секторе речь даже не заходит. Тем не менее, такие заказчики с большим интересом относятся к аналоговому видеонаблюдению высокого разрешения.

Видеонаблюдение в любых погодных условиях — уже реальность. Имеются камеры, способные формировать изображение в условиях фронтальной засветки прямыми солнечными лучами, не жертвуя при этом уровнем детализации в сцене, и камеры, способные формировать цветные изображения в почти полной темноте. Камеры могут эффективно отстраиваться от вибрационных колебаний, ударов и даже от тумана.

Социальные сети и видеонаблюдение. Эксперты компании *IHS Technology* считают, что повсеместное распространение смартфонов, оборудованных встроенными телекамерами и средствами подключения к Интернету, в сочетании с развитием популярных социальных сетей, привело к тому, что сообщество пользователей впервые в истории сетей сумело создать единую базу видеоматериалов, пригодную для использования в интересах полицейских расследований, — по сути, именно это явление и носит название краудсорсинга. Эта тенденция в видеонаблюдении также будет развиваться в ближайшие годы.

По оценке экспертов компании *Cisco*, пользовательский трафик в Интернете достиг в 2017 году 1,4 зеттабайт (1,4·1021) – а суммарный объём загружаемых в сеть с мобильных устройств

видеоданных в 2012-2017 годах вырос в 16 раз, и его доля составляет 2/3 всего мирового мобильного трафика.

Видеонаблюдение в сфере обеспечения безопасности жилища. *Периметровые камеры* позволяют осуществлять верификацию тревог, поступающих от сенсоров охранной сигнализации, — это даёт возможность избежать ложных тревог и связанной с ними необходимости обращаться в правоохранительные органы. Также растёт спрос на услуги удалённого хостинга со стороны домовладельцев.

Эксперты в области безопасности, опрошенные американским журналом *SDM*, единодушны в том мнении, что рынок видеонаблюдения остаётся сильным – и что его рост будет продолжаться. В числе способствующих этому росту факторов следует отметить большее количество приложений для видео, более высокую интеграцию – и несколько технологий, получающих большее распространение, таких как аналитика, «большие данные» (*big data*) и других.

Тем не менее, в 2018 году этот рост может несколько замедлиться – отчасти из-за снижения цен на камеры, насыщенности рынка и выравнивания перехода от аналоговых к IP технологиям.

Рыночные драйверы. Одним из факторов, который всегда управляет рынком, — это требование о соответствии, в особенности, когда конечные пользователи не соответствуют необходимым требованиям. На вертикальных рынках существует множество драйверов соответствия, таких, как коммунальные услуги и здравоохранение.

Ещё одним драйвером на рынке видеонаблюдения являются технологические достижения и взаимосвязь различных технологий, которые никогда не пересекались друг с другом. Речь идет о перспективе использования датчиков и устройств в

сфере «Интернета вещей», предоставляя клиентам эффективные инструменты для управления рынком.

Текущие угрозы, будь то киберпреступность или терроризм, представляют собой вполне очевидный третий драйвер, степень воздействия которого сложно переоценить. Растёт интерес со стороны клиентов к аналитическим технологиям и, в частности, бизнес-аналитике. По данным исследовательской компании *MarketsandMarkets*, рост рынка *VSaaS* в 2018 году должен составить 10%.

Видеосервисы на данный момент присутствуют в портфолио двух из трёх крупных интеграторов и поставщиков программных решений – зачастую в качестве технического фундамента к другим системам (обеспечение доступа и оперативного реагирования). Другой проблемой может быть то, что переход индустрии к IP-технологиям почти завершён. Рынок IP-решений, способных интегрироваться с другими системами, в течение ближайших лет будет расти.

Пользователи возвращаются к более известным и проверенным брендам производителей IP-камер, внедряющих в сетевые устройства протоколы кибербезопасности. В 2018 году видеобезопасность является основным направлением для всех поставщиков продуктов, интеграторов и конечных пользователей.

По прогнозам *IHS Markit*, 75% всех серверов с *глубоким обучением (deep learning)* для видеонаблюдения, отправленных по всему миру в 2018 году, поставлены из Китая. Ожидается, что рынок видеонаблюдения как услуга (*VSaaS*) будет расти со значительными темпами, более чем на 10%. При этом главный спрос связан с розничной торговлей, малыми предприятиями и жилыми приложениями. *VSaaS* предлагает основные преимущества использования любого устройства, таких как

ноутбуки, смартфоны и настольные компьютеры, для удаленного доступа к видеопотокам, хранящимся в «облаке».

Поскольку разрешение видео постоянно улучшается, его сжатие становится всё более важной задачей. Внедрение стандарта *H.264* дало импульс для распространения мобильного видео. Ныне в отрасли с нетерпением ожидают появления стандарта *H.265*, который должен стать следующим шагом в более эффективном сжатии видеофайлов. H.265 превосходит стандарты сжатия *Google* и внутренний протокол сжатия *Amazon*.

Ещё одна возможность, предоставляемая более дешёвыми камерами, — это более широкая аудитория для видео.

Востребованная в Европе конфиденциальность. Конфиденциальность и её защита абсолютно важна в европейских странах, особенно в Германии и Скандинавии.

Перспективы хранения данных для видеонаблюдения в 2018 году. В 2017 году развитие в странах Европы и Северной Америки получила бизнес-модель видеонаблюдения как услуги (*VSaaS*). Кроме того, нельзя не отметить очевидный технологический прогресс видеокамер и другого оборудования. При этом поставщиками услуг сделан упор не просто на стандартный мониторинг, а на видеоаналитику – в частности, считывание биометрических данных.

FCX.iQ

Решение для проведения операций обмена валют

FCX.iQ
.iQ Family Product

FCX.iQ - решение, позволяющее проводить операции обмена валют на банкоматах Diebold Nixdorf, а также другие возможности для расширения функциональности устройств самообслуживания: поддержку работы бесконтактных карт, выполнение различных платежных операций и адаптацию терминалов для людей с нарушениями зрения.

Глава 2. Видеоаналитика: аппаратное и программное обеспечение

«Вообще трудно было рассчитывать на то, что за городом безопаснее, чем в Лондоне. Телекранов, конечно нет, но в любом месте может скрываться микрофон – твой голос услышат и опознают…»

Дж. Оруэлл, «1984»

Видеоаналитика (*video analytics*, или *video content analysis*) — это направление, в рамках которого с помощью методов компьютерного анализа видеоконтента формируются результирующие данные о наблюдаемых объектах. Видеоконтентом может быть серия изображений, поступающих с камер в режиме реального времени или архива видеозаписей.

Использование видеоаналитики повышает эффективность системы видеонаблюдения, снижая нагрузку на сотрудников службы безопасности и управления, и помогает полностью оценить качество видеоизображения, сделав систему IP-камер более интеллектуальной в своей работе. Это осуществляется с помощью алгоритмов различения типов объектов и выявления определённого поведения или действия в режиме реального времени, предоставления оповещений и различных сведений для пользователей.

На практике видеоаналитика реализуется специальным аппаратным и/или программным обеспечением, не требующим непосредственного участия человека. Алгоритмы видеоаналитики могут быть интегрированы в различные бизнес-системы, в том числе, в системы видеонаблюдения.

В качестве примера задачи видеоаналитики можно привести оценку параметров движения по серии снимков трёхмерной (3D) сцены: оценки скорости конкретной области на снимках, или определение трёхмерного движения камеры.

В рамках видеоаналитики обеспечивается автоматизированное выполнение следующих функций:

- *Обнаружение* - видеоданные проверяются на выполнение поставленных условий. Например, обнаружение, основанное на быстрых вычислениях, может использоваться для нахождения небольших областей в анализируемом изображении, которые затем подлежат анализу с помощью алгоритмов интерпретации, более требовательных к машинным ресурсам.

Содержание может быть определено, например, в терминах схожести с конкретным изображением, или в терминах высокоуровневых текстовых критериев поиска (например, поиск всех снимков, снятых зимой на фоне домов, вблизи которых нет машин).

- *Оценка положения или ориентации* конкретного объекта относительно камеры. Опасные ситуации в видеопотоке с камер наблюдения (например, скопления людей, оставленные предметы, возгорания и задымления и т. п.). При возникновении проблемы требуется передать сообщение на пульт охраны и указанные мобильные устройства, осуществляя при этом документальную запись видео и протокола событий.
- *Слежение* (следование за перемещениями объекта в зоне наблюдения, например, людей или машин).
- Распознавание или идентификация отдельного экземпляра объекта наблюдения. Под распознаванием можно понимать широкий спектр задач — от классификации объекта на цель/шум до идентификации

или верификации объекта по биометрическим признакам. Примерами могут служить идентификация лица конкретного человека или его отпечатков пальцев.

Указанные функции выполняются многократно в целях непрерывного уточнения гипотез о количестве, местоположении и типах объектов в зоне наблюдения, а также устранения избыточности в результатах.

При использовании средств видеоаналитики ответы на многие вопросы, в том числе, «Где именно будет проводиться анализ?», придётся давать неоднократно. [4].

2.1. Обнаружение движения и его анализ

Программное обеспечение для видеоаналитики для камер безопасности доступно в нескольких видах: оно может быть установлено на камере потребителя, на устройстве NVR или в качестве программного обеспечения сторонних производителей. Локально устанавливаемые приложения являются масштабируемыми, сокращая трафик и объём памяти для хранения записей. Это достигается благодаря записи и отправки лишь тех фрагментов видео, которые представляют реальный интерес.

Например, многие предприятия розничной торговли используют системы наблюдения для обнаружения движения в торговых залах после их закрытия. Можно настроить систему на обнаружение движения в часы после закрытия, поэтому при обнаружении движения на пульт охраны будет отправлено сообщение для реагирования.

Передний план – это область на кадрах, где происходят события в зоне наблюдения. Для его выделения применяются специализированные алгоритмы сегментации, и каждый из полученных сегментов исследуется по отдельности. Например, такой алгоритм может произвести поиск участков, соответствующих типичным образцам – головы, глаз, плеч и т.д. Обнаружив участок «голова», алгоритм будет вести, в его пределах, поиск положения глаз, а на определённых расстояниях – других частей тела человека. При отсутствии таких «значимых» участков алгоритм откажется от гипотезы об обнаружении «головы» и перейдёт к следующей гипотезе. При сопоставлении двух последовательных кадров или текущего кадра с накопленным (усреднённым по времени) *фоном* может быть сформировано разностное изображение. Используя это изображение (*маску)*, можно выделить движущиеся объекты на переднем плане.

Обнаружение движения (*Motion Detection*). Практически все нынешние сетевые камеры имеют встроенные средства обнаружения движения.

Анализ или трекинг движения (*Motion Tracking*). При трекинге в наблюдаемой сцене осуществляются выделение и анализ перемещений объектов. Для этого применяются алгоритмы, основанные на запоминании текущего кадра в качестве фона и непрерывном анализе изменений. При сравнительном анализе соседних кадров все движения на переднем плане можно отделить от запомненного накопленного фона.

Различие между простым обнаружением и анализом движения состоит в том, что, если в первом случае выявляется наличие отличий содержания текущего кадра от предшествующих, то во втором случае целью является обнаружение объектов в пределах относительно небольших участков, изменчивость которых соответствует определённым логическим условиям.

2.1.1. Стереоскопическое восприятие

Во многих приложениях важное значение имеют трёхмерная природа как объекта в сцене, так и процесса съёмки изображения.

Такие задачи, как определение местоположения объекта наблюдения относительно камеры или выделение закрытых, или частично загороженных объектов, требуют привлечения информации о трёхмерной сцене. Эта информация может стать вспомогательным средством для двумерного анализа сцен [3].

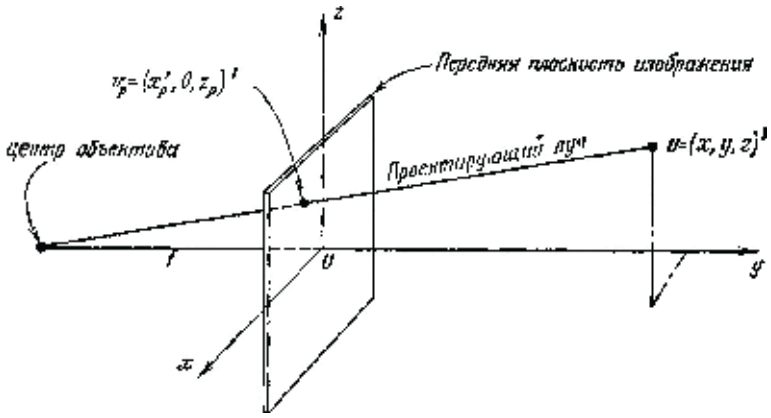
Возможности алгоритма анализа трёхмерных сцен часто могут быть расширены за счёт использования некоторых математических свойств процесса съёмки изображения. Интерес представляют как методы ответа на вопросы, требующие сами по себе информации о трёхмерной сцене, так и методы, использующие информацию о трёхмерной сцене в качестве вспомогательного средства для двумерного анализа. Оба вида задач решаются в рамках одной математической модели.

Как известно, *перспективное преобразование* – это процесс отображения многих точек в одну, что означает, что по заданной точке изображения невозможно однозначно определить положение соответствующей ей точки объекта.

Метод получения дополнительной информации на основе двух изображений, необходимой для достижения однозначности, называется *стереоскопией*.

Хотя каждой точке объекта соответствует только одна определённая точка изображения, все точки объекта, расположенные на линии, которая проходит через центр объектива, имеют один и тот же образ. Таким образом, для каждой точки изображения существует в пространстве линия,

определённая этой точкой изображения и центром объектива, и на этой линии должна лежать соответствующая точка объекта (ил.1).



Ил. 1. Модель камеры с передней плоскостью изображения.

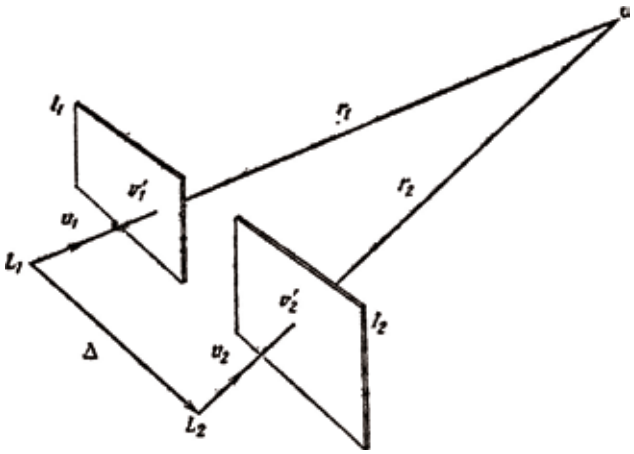
Таким образом, возникают две важные задачи, связанные с процессом съёмки изображения:

- для любой данной точки объекта определить местоположение её образа на изображении;
- для любой данной точки изображения определить, где расположена прямая линия, на которой должна лежать соответствующая точка объекта.

Решение этих задач можно получить с помощью прямого и обратного перспективных преобразований [3]:

$$x_p = \frac{fx}{f+y},$$
$$y_p = 0,$$
$$z_p = \frac{fz}{f+y}. \qquad , \qquad x = \frac{x_p}{f}(y+f) = \frac{x_p}{z_p}z,$$

Упрощённая схема для стереоскопического восприятия показана на ил. 2. На ней показаны две плоскости изображений I1 и I2, два центра объективов L1 и L2 и два проектирующих луча r1 и r2, проведённых между соответствующими центрами объективов и точкой v объекта. Вектор $\Delta = L_2 - L_1$ называется базовым вектором; его длина называется просто базой.



Ил.2. Основная схема для стереоскопического восприятия

Вычисления, связанные со стереоскопией, состоят из двух частей. Во-первых, должно быть определено расположение двух точек на каждом изображении, v1 и v2, соответствующих точке v объекта. Во-вторых, с помощью тригонометрических вычислений надо найти точку пересечения двух проектирующих лучей. Первая задача, называемая определением соответствия, обычно решается одним из двух способов. Простейший способ состоит в том, чтобы определить, используя то или иное средство, положение образа точки v на каждом изображении. Однако часто легче определить положение образа точки v на одной из картинок, а затем использовать процедуру сравнения с эталоном, чтобы обнаружить соответствующий образ на другой картинке. В частности, пусть сначала определяется положение точки v1.

Затем, поскольку мы ищем точку (или небольшую область) плоскости I_2, которая соответствует точке v, мы используем в качестве эталона небольшую область плоскости с центром в точке V'_1

Эталон, построенный таким образом, перемещается по плоскости I_2 до тех пор, пока не будет найдено соответствие.

2.1.2. Калибровка

Рассмотренные перспективные преобразования включают ряд геометрических параметров. Даже в простейшем случае, чтобы преобразование было определено полностью, должно быть известно расстояние от плоскости изображения до объектива с точечным отверстием. Неточности при задании позиции камеры могут привести к нежелательным ошибкам при определении местоположения объектов наблюдения.

Хотя некоторые параметры могут быть измерены непосредственно, на практике обычно удобнее определить, по крайней мере, часть из них, используя саму камеру в качестве измерительного инструмента. Основная идея заключается в том, чтобы присвоить параметрам такие значения, которые сведут до минимума разницу между измеренными и вычисленными положениями точек картинки.

Для решения реальных задач видеоаналитики применяют *внешнюю и внутреннюю калибровку* камер.

Внешняя калибровка включает в себя установку параметров, задающих общее начало системы координат и положение камеры в мировых координатах, высоту установки камеры и угол поля зрения объектива.

На практике, в целях избегания ошибок производится взаимная калибровка камер – на изображениях фиксируются точки с известными координатами.

Перспективная калибровка - достаточно надёжный метод внешней калибровки: с его помощью можно задать характерные для сцены соотношения размеров объектов. Для этого вручную задаются пиксельные размеры людей, транспортных и иных технических средств – раздельно в верхней и нижней частях изображения. Благодаря этому удается различать людей и другие объекты с близкими пиксельными размерами, по геометрическим пропорциям, характеру движения и т.д.

Внутренняя калибровка обеспечивает корректировку геометрических искажений изображения. Камера искажает не только углы, но и пропорции размеров объектов в сцене. При этом каждая камера должна проходить внутреннюю калибровку в отдельности. Для коррекции геометрических искажений в сцену наблюдения помещают специальный калибровочный объект.

2.2. Многооконный мониторинг (*Multi View*)

Если видеоаналитика применяется для определения местоположений на карте, точность решения этой задачи в значительной степени зависит от позиционирования камер. Если камеры направлены под небольшими углами к горизонтали, погрешность будет относительно высокой. Также ошибки аналитики могут привести к существенным отклонениям автоматически определяемых координат объектов от их реального местоположения.

В настоящее время на рынке предлагаются различные средства для многооконного мониторинга. Например, устройство

Blackmagic MultiView 4 компании *Blackmagic Design* обеспечивает одновременный вывод на один экран четырех независимых SDI-сигналов. На каждом входе *6G-SDI* выполняется полная повторная синхронизация, благодаря чему можно работать с комбинацией *SD*-, *HD*- и *Ultra HD*-форматов любой кадровой частоты. Это устройство, имеющее поддержку *1080 HD* и *2160p Ultra HD*, совместимо с *HD*- и *Ultra HD*-дисплеями. При подключении *Ultra HD*-телевизора или монитора изображение в каждом окне отличается исключительно высокой резкостью, так как его разрешение составляет 1920X1080 HD. Дополнительно можно использовать индикаторы уровня звука и идентификаторы окон.

Также может оказаться полезным поисковое средство *MomentQuest* компании *AxxonSoft*, которое применяется для быстрого нахождения в видеоархиве лиц, автомобильных номеров и событий по заданным критериям. Поиск и мониторинг ведутся по метаданным, которые автоматически вычисляются для всех попавших в кадр движущихся объектов и сохраняются в базе данных одновременно с записью видео.

Для осуществления возможности поиска по лицам система в качестве метаданных сохраняет биометрический вектор (краткое описание лица) всех присутствующих в кадре людей. При последующем поиске пользователь может загрузить в систему фотографию искомого лица.

Все номера транспортных средств, появляющиеся в поле зрения видеокамер, сохраняются в базе данных в текстовом виде. Впоследствии пользователь в качестве критерия поиска может ввести номер необходимого автомобиля.

Для поиска интересующих событий пользователю достаточно задать параметры поиска, и система в считанные секунды найдёт все видеозаписи, соответствующие этим параметрам.

2.3. Шаблоны поведения

Как правило, автоматизированное обнаружение потенциально опасных ситуаций осуществляется на основе известных шаблонов поведения, типичных для данной сцены при конкретной оперативной обстановке. Формализованное описание поведения для сопоставления его шаблоном поведения строится по имеющимся данным с установленных детекторов.

Отметим, что в разделе 3.2.1 описаны сценарии по выявлению нежелательных или подозрительных ситуаций с помощью распознавания лиц для устройств самообслуживания в комплексе с системой *ATMeye.iQ*.

Другими примерами такого рода являются применения модулей *Security Manager* (менеджер по безопасности) и *Fraud Detection* (обнаружение мошенничества) в программном комплексе *Vynamic Security* компании *Diebold Nixdorf*.

Модуль *Security Manager*, предназначенный для обнаружения мошенничества на основе шаблонов событий и корреляции событий и управления паролями *BIOS*, дополняет имеющиеся функции.

Модуль *Fraud Detection*, используя технологии *Big Data* и машинного обучения, обеспечивает отслеживание отклонений в стандартных сценариях поведения программ, процессов и пользователей. Информация о подобных аномалиях в режиме реального времени доводится до сотрудников службы безопасности, после чего ответственный персонал может запустить один из сценариев для защиты информации, денежных средств и имущества финансового учреждения.

2.4. Аппаратное обеспечение для видеоаналитики

Как правило, в современных камерах применяются счётчики различных видов и алгоритмы расширенного обнаружения движения. Выходные результаты этих алгоритмов превосходят аналогичные показатели от типичных детекторов движения. Нынешние «умные» камеры обладают значительно большей функциональностью по сравнению с такими детекторами движения.

К примеру, система видеонаблюдения «Интеллект» компании *AxxonSoft* использует детекторы трёх видов: базовые, ситуационные и сервисные.

Базовые детекторы. Группа детекторов движения предназначена для обнаружения движущихся объектов в кадре. Базовый детектор определяет наличие движения без дополнительных условий. Трекер выявляет наличие движения и его направление, может вести объекты в условиях тряски. Инфракрасный детектор (для его работы требуется тепловизор) определяет наличие движения в инфракрасном диапазоне, а детектор направления движения обнаруживает движение в заданных направлениях.

Детектор оставленных/исчезнувших предметов оповещает о появлении в кадре предмета или исчезновении предмета из кадра. Детектор позволяет обнаружить, например, исчезновение ноутбука со стола, оставленный в холле здания «дипломат» или неправильно припаркованный автомобиль.

Детектор лиц обнаруживает появление в кадре лица человека, отличая его от любого другого объекта.

Ситуационные видеодетекторы предназначены для определения заданных типов перемещений объекта в кадре. При задании пользователем линии, многоугольных зон и

временных интервалов система выявляет события, соответствующие заданным критериям события.

Ситуационные видеодетекторы определяют:

- пересечение объектом прямой линии в выбранном направлении;
- пересечение объектом ломаной линии в выбранном направлении;
- движение в зоне;
- вход объекта в зону;
- выход объекта из зоны;
- появление объекта в зоне;
- исчезновение объекта в зоне;
- остановка объекта в зоне;
- пребывание объекта в зоне более 10 секунд;
- оставленный в зоне предмет.

Любой из детекторов можно настроить на работу с определённым типом объектов: человек, автомобиль или все объекты.

Сервисные детекторы подают сигнал в случае сбоев в работе видеокамер. Они позволяют не только идентифицировать попытки вывода камер из строя, но и выявляют различные помехи, мешающие качественной регистрации событий.

Детектор закрытия объектива определяет все случаи непреднамеренного или преднамеренного закрытия объектива. Он особенно важен в ситуациях, когда телекамера расположена в пределах досягаемости.

Детектор засветки подаёт сигнал в том случае, когда в объектив направлен луч яркого света, например, фонарика, прожектора или фар автомобиля.

Детектор сдвига камеры оповещает о манипуляциях по переориентации камеры в пространстве. Детектор особенно востребован в ситуациях, когда камера находится в пределах досягаемости человека, и её легко можно повернуть.

Детектор изменения фона реагирует на изменение фона перед камерой. Этот детектор очень похож на предыдущий, но при этом решает несколько иные задачи. Если детектор сдвига реагирует на манипуляции с самой телекамерой, то детектор изменения фона — на манипуляции вокруг неё, например, на попытку установить перед камерой искусственный фон.

Детектор расфокусировки оповещает о потере чёткости изображения в результате расфокусировки объектива камеры или его загрязнения, например, в том случае, если кто-либо умышленно или по неосторожности сбил фокус.

Стоит также перечислить основные отличия видеодетектора в системе *HD* по сравнению с системами стандартной чёткости [15]:

- более значительная детализация сцены *HD* приводит к учащению ложных срабатываний. Собственные движения камеры, обусловленные ветром и вибрацией техники, становятся причиной значительных изменений изображения. Применение цифрового или механического стабилизатора изображения становится обязательным;
- мегапиксельные камеры имеют большую дальность действия или радиус обзора. Диапазон масштабов объектов может быть более широким по сравнению с системами *SD*. В системах *HD* необходимо применять принципиально другие алгоритмы перспективной калибровки и оптической коррекции, а также использовать многомасштабные алгоритмы моделирования фона и сегментирования объектов;

- поток данных в системах HD многократно превышает поток данных в системах *SD*. Большинство алгоритмов, используемых в интеллектуальных видеодетекторах, обладают нелинейной сложностью по отношению к размеру кадра, и нагрузка на процессор возрастает на несколько порядков. Таким образом, необходимо принципиально оптимизировать и создавать новые алгоритмы для работы с потоком *HD*.

2.5. Программное обеспечение для видеоаналитики

Программное обеспечение для видеоаналитики предназначено для помощи при просмотре растущего числа часов видеонаблюдения, которые, возможно, никогда не удалось бы полностью осуществить охранной службой или системным менеджером. Следует помнить, что система видеонаблюдения будет настолько полезной, насколько удастся фактически захватывать и просматривать инциденты, в чём видеоаналитика и окажется полезной.

Видеоаналитика входит в число инновационных технологий, предлагаемых сегодня поставщиками средств управления видео и видеоинформационными инструментами (*video management system; VMS*).

Программное обеспечение для видеоаналитики для камер безопасности может быть установлено на камере или видеорегистраторе, или в качестве программного обеспечения сторонних производителей.

Решения для видеоаналитики будут работать по-разному в зависимости от производителя и сферы приложения. Хотя все

они функционируют примерно одинаково, при настройке программного обеспечения нужно настраивать параметры для работы программного обеспечения, а также настроить систему уведомлений о предупреждениях. Всякий раз, когда программное обеспечение обнаружит что-либо, соответствующее критериям поиска этой системы, оно будет предупреждать об этом.

Например, многие компании используют системы наблюдения для обнаружения движения в своих офисах после окончания работы. Для этого можно настроить систему на обнаружение движения в часы, когда офис закрыт – поэтому, когда система обнаружит движение, она отправит сообщение об этом соответствующим службам.

В настоящее время для создания полноценных систем видеоаналитики предлагаются различные программные решения.

OpenCV (*Open Source Computer Vision Library*). Эта библиотека программ выпускается под лицензией BSD и, следовательно, бесплатна как для академического, так и для коммерческого использования. Она имеет интерфейсы *C ++,* C, *Python, MATLAB* и *Java* и поддерживает операционные системы *Windows, Linux, Mac OS, iOS* и *Android* [11].

Библиотека состоит из программ компьютерного зрения с открытым исходным кодом и компьютерного обучения на оптимизированном *C/C++*.

OpenCV был создан для обеспечения общей инфраструктуры приложений для компьютерного зрения и ускорения использования машинного восприятия в коммерческих продуктах. Он отличается вычислительной эффективностью и с большим вниманием к созданию приложений реального времени.

С помощью включённого в комплект открытого языка вычислений *OpenCL* библиотека *OpenCV* может воспользоваться аппаратным ускорением базовой гетерогенной вычислительной платформы.

Принятая во всем мире *OpenCV* имеет более 47 тыс. пользователей сообщества пользователей, а количество его загрузок превышает 14 млн.

Библиотека насчитывает более 2500 оптимизированных алгоритмов, включающих в себя полный набор классических и современных алгоритмов компьютерного зрения и машинного обучения. Эти алгоритмы могут использоваться для обнаружения и распознавания лиц, идентификации объектов, классификации действий человека в видео, отслеживания движения камеры, отслеживания движущихся объектов, извлечения *3D*-моделей объектов, создания *3D*-облаков точек из стереокамер, «сшивания» изображений вместе для получения высокого разрешения изображение всей сцены, поиска схожего изображения из базы данных изображений, удаления «красных глаз» (*red eyes*) с изображений, сделанных с помощью вспышки, слежения за движениями глаз, распознавания сцен и установки маркеров (для наложения их на дополненную реальность) и т. д. Библиотека широко используется в компаниях, исследовательских группах и правительственных органах.

Наряду с известными компаниями как *Google, Yahoo, Microsoft, Intel, IBM, Sony, Honda, Toyota*, которые используют библиотеку, *OpenCV* также широко применяют многочисленные стартапы.

Сфера применения *OpenCV* охватывает диапазон от «сшивания» вместе изображений уличного обзора, обнаружения вторжения в систему видеонаблюдения в Израиле, контроля оборудования шахт в Китае, выявления несчастных случаи в бассейнах в Европе до запуска центра интерактивного искусства в Испании

и Нью-Йорке, проверки чистоты взлётно-посадочных полос в Турции, проверки этикеток на продуктах на заводах во всём мире, быстрого выделения лиц (по видео) в Японии.

Не так давно *Microsoft* внесла в инструменты по искусственному интеллекту (ИИ) для компаний ряд улучшений, связанных с распознаванием лиц и объектов, а также классификацией изображений [20]. Все обновления являются частью набора *application programming interface* (*API)* под названием *Cognitive Services*, с которых разработчики смогут интегрировать в свои продукты интеллектуальные функции, даже если у них нет опыта работы с искусственным интеллектом.

С помощью платного инструмента *Custom Vision Service* компании могут обучать свои системы классификации изображений определённым задачам — например, определению различных видов птиц или различению разновидностей фруктов, — без необходимости создавать собственные модели искусственного интеллекта. Модели, созданные с помощью *Custom Vision Service*, можно экспортировать из «облака» *Microsoft* и разворачивать на смартфонах.

Face API теперь можно обучать на базе 1 млн лиц, благодаря чему технология стала существенно точнее различать людей.

Наконец, стал общедоступен *Bing Entity Search*. Сервис, использующий базу данных поискового движка *Microsoft*, позволяет вести поиск известных людей, места и предметы – и получать о них соответствующую информацию.

В завершении отметим мощную платформу безопасности и видеомониторинга устройств самообслуживания *ATMeye.iQ*, которая находится в центре внимания этой книги.

Поэтому далее будут рассмотрен ряд известных на рынке программных решений для видеоаналитики других производителей.

2.5.1. Приложения *AXIS Video Motion Detection* (Детектор движения и видеозапись)

Приложения видеоаналитики *AXIS* позволяют проводить проактивное наблюдение, помогая сотрудникам службы безопасности при обнаружении и предотвращении противоправных действий. Приложения могут, например, обнаруживать нарушителей и автоматически уведомлять охранника или воспроизводить сообщение через громкоговоритель. Эти приложения масштабируемы, помогают сократить пропускную способность и использование хранилища, отправляя и записывая лишь то видео, которое представляет интерес.

Например, *AXIS Video Motion Detection 4* — это бесплатное приложение видеоаналитики, установленное в большинстве сетевых камер и видеокодеров *AXIS*. Приложение отправляет сигналы тревоги при обнаружении движения в случае движущихся объектов — людей и автомобилей — в пределах заданных областей. Кроме того, приложение позволяет уменьшить трафик и объём памяти для хранения данных, поскольку видеозапись включается в камерах только при возникновении движения.

Приложение работает в различных условиях освещения — как внутри помещений, так и на улице. Оно окажется особенно полезным в местах с малой интенсивностью движения — например, в коридорах офисов, на автомобильных стоянках, в неконтролируемых местах торговых точек и для видеонаблюдения после окончания рабочего дня.

В качестве другого примера можно привести открытую платформу *AXIS Camera Application Platform* (*ACAP*), поддерживаемую большинством камер *AXIS*. Платформа

позволяет добавлять средства аналитики и другие приложения в зависимости от конкретных требований безопасности и бизнеса. Приложения полностью готовы для непосредственного применения в устройствах *AXIS* с целью анализа «живого» видео и видеозаписей. Примерами могут являться приложения для обнаружения пересечения заданной линии, подсчёта людей, распознавания номерного знака автомобиля и т. д.

2.5.2. Видеоаналитика на платформе *Axxon Next*

Компания *AxxonSoft* - известный разработчик интеллектуальных интегрированных систем безопасности и видеонаблюдения. Платформы *AxxonSoft VMS* и *PSIM* обеспечивают более 240 проектов муниципального надзора *Safe City* и систем безопасности в розничных сетях, банках, аэропортах, портах, промышленных объектах и т.д. во всём мире.

Axxon Next – последующее поколение программ для управления видеонаблюдения с открытой платформой (*VMS*). Системы видеонаблюдения на базе *Axxon Next* могут масштабироваться без ограничений на количество видеосерверов, рабочих станций или видеокамер.

Система *Axxon Next* включает видеодетекторы движения, изменения фона, потери качества видеоизображения, оставленных предметов, пересечения линии в выбранном направлении, начала и прекращения движения, появления объекта и т.д.

Платформы *Axxon* способны подключаться к хранилищу, встроенному в камеры, при этом имеется возможность. смотреть, экспортировать и копировать видео с SD-карт.

Имеющиеся инструменты анализа поступающей видео- и аудиоинформации позволяют *Axxon Next* распознавать самые различные заданные пользователем ситуации. В качестве реакции на срабатывания детекторов или подключённых к камерам охранных датчиков можно выбрать одно или несколько действий из списка:

1. включить запись видео с камеры (со звуком);
2. отправить *SMS*-сообщение на один или несколько номеров;
3. отправить электронное письмо на один или несколько адресов;
4. воспроизвести звуковое сообщение;
5. подать сигнал на подключённое к камере исполнительное устройство (реле);
6. перейти в режим обработки тревог;
7. повернуть поворотную камеру в заданном направлении.

Должным образом настроенная система требует минимального вмешательства в её работу, фиксируя при этом все важные события в видеоархиве и привлекая внимание оператора к тревожным событиям.

В системе обеспечена поддержка более 6000 моделей *IP*-устройств (включая более 1500 моделей *IP*-камер, интегрированных с использованием проприетарного протокола и 4500 совместимых с *ONVIF*-устройств), а также удалённый доступ с мобильных устройств и веб-интерфейс.

Axxon Next включает развитую систему анализа видеоизображений, в том числе, следующие средства обнаружения:

- обнаружение движения (фиксирует любое движение в сцене);
- обнаружение фонового изменения (срабатывает при попытке поворота камеры);

- обнаружение потери качества видео (срабатывает, когда качество изображения ухудшается из-за размытия, загрязнения или ослепления объектива или изображения и т.д.);
- обнаружение оставленных объектов (срабатывает, когда на сцене появляется некоторый объект – портфель, коробка, сумка и т.д. – и остаётся неподвижным в течение некоторого времени);
- обнаружение пересечения линии в заданном направлении (срабатывает, когда движущийся объект пересекает виртуальную линию в заданном пользователем направлении; доступно в платной версии);
- обнаружение начала движения (запись движения в заданной пользователем области);
- обнаружение остановки движения (срабатывает, когда любой объект останавливается и остаётся неподвижным в течение некоторого времени в пределах указанной пользователем области);
- обнаружение ситуации, когда объект остается в определённой пользователем области в течение некоторого времени;
- обнаружение появления объекта (срабатывает, когда какой-либо объект появляется в заданной пользователем области);
- обнаружение исчезновения объекта)срабатывает, когда объект покидает указанную пользователем область – или когда объект, расположенный в пределах области, исчезает из поля зрения камеры).

В дополнение к средствам видеообнаружения *Axxon Next* имеет два аудиодетектора:

- обнаружение шума (срабатывает за счёт превышения определённого порогового уровня громкости);

- обнаружение тишины (срабатывает, когда сигнал с микрофона полностью пропадает).

Инструменты для анализа входящих видео и аудиоданных позволяют *Axxon Next* распознавать различные пользовательские ситуации.

Инструменты видеообнаружения *Axxon Next* сконфигурированы в визуальном режиме. После указания областей, линий и других параметров операции инструмента внутри сцены и нажатия ***Apply***, пользователь сразу увидит, как этот инструмент обнаружения будет работать с потоком видео, поступающим с камеры, – все сцены, которые запускали инструмент, будут отображаться в режиме реального времени в специальной области экрана.

2.5.3. Программное обеспечение *Milestone XProtect*

Компания *Milestone* известна [14] своим новейшим программным обеспечением для средств управления видео и видеоинформационными инструментами, которые повышают производительность *IP*-видео.

Milestone XProtect – это ведущая платформа *VMS* от *Milestone*, которая может быть смешанной и совместимой с многочисленными *IP*-камерами и моделями видеорегистраторов (*NVR*) для универсального развёртывания.

Для получения доступа к *Milestone XProtect VMS* «на ходу» созданы приложения *iPhone Milestone*, предоставляющие полный контроль с нескольких сайтов над имеющимися *IP*-камерами. Благодаря этому отпадает необходимость отслеживать канал камеры непосредственно «на месте».

Milestone XProtect Mobile имеет три приложения для смартфонов, совместимых с *iPhone, Android* и *iPad*. С помощью этих приложений для мобильного мониторинга можно следить за *IP*-камерами, воспроизводить записанное видео, отправлять снимки по электронной почте и *MMS*, а также выполнять поиск в видеоархиве.
Программное обеспечение для управления видео *Milestone* позволяет интегрировать большой набор надстроек *Milestone*, а также поддерживаемые аппаратные и сторонние приложения.

Программное обеспечение *Milestone* для видеоаналитики поставляется со множеством функций, благодаря чему можно легко вписаться в любую систему наблюдения.

2.5.4. Видеоаналитика на платформе *VideoNet*

Российская компания-производитель «СКАЙРОС» (Санкт-Петербург) с 1996 года предлагает на рынке интегрированную платформу безопасности *VideoNet*.

Система обладает стандартными функциями – такими, как обнаружение движения, фиксирование оставленных предметов, подсчёт объектов, проходящих через зону видимости камеры, реагирование на изменение направления движения объектов, фиксирование пересечения линии и т.п.

Последняя версия этой платформы – *VideoNet 9 Prime*, с помощью которой можно создать профессиональную систему сетевого видеонаблюдения. Данное решение обеспечивает управление видео от 1 до 16 *IP*-камер, производить запись по камерам, использовать различные настройки и сценарии, осуществлять мониторинг и контроль ситуации и происшествий с компьютера, планшета, смартфона из любой точки мира.

Реализованные в платформе *VideoNet* алгоритмы анализа видеоизображения обнаруживают тревожные события и

минимизируют ложные срабатывания. Благодаря этому можно записывать лишь необходимую информацию, сэкономить на размере архива. Также упрощается дальнейший поиск информации в архиве за счёт формирования метаданных вместе с записью видеопотока.

В системе *VideoNet* применяются интеллектуальные детекторы, которые в автоматическом режиме выявляют и реагируют на подозрительные и опасные события. Для каждой камеры можно создать несколько комбинаций из разных детекторов, различные комбинации зон детектирования с индивидуальными параметрами для каждой из этих зон.

Так, нейросетевой детектор определения типов объектов обеспечивает однозначную идентификацию в кадре следующих типов объектов: человек, автомобиль, автобус, мотоцикл, велосипед, собака, поезд, самолёт.

Нейросетевой детектор определения типов объектов относится к категории детекторов, использующих алгоритм распознавания объектов, в основе которого лежат *свёрточные нейронные сети* [23].

Если система зафиксирует объект заданного типа в поле зрения камеры, транслируемой в видеоокне, то на видеоизображении с камеры объект будет обведен прямоугольником с отметкой о его типе и номере в очереди.

Предусмотрена возможность настроить автоматическую реакцию на наступление события от детектора – например, включить видео- и аудиозапись, отправить *SMS*-сообщение или электронное письмо, сохранить кадр, запустить архивирование, приложение или звуковое сообщение, создать отчёт, отправить команду на исполнительное устройство, и многое другое.

2.5.5. Видеоаналитика из «облака» на базе *VisionLabs LUNA*

В декабре 2017 года российская компания «КРОК» выпустила на рынок «облачную» систему видеоаналитики, реализованную на базе платформы *VisionLabs LUNA* в формате управляемого сервиса. Она доступна из «облака» «КРОК» – и может использоваться в условиях отсутствия у заказчика собственной *ИТ*-инфраструктуры.

Сервис позволяет в режиме реального времени извлекать из видеопотока важную для бизнеса информацию и передавать её другим корпоративным системам либо непосредственно бизнес-пользователю в виде разнообразных отчётов. Решение не только выделяет и распознаёт на видео отдельные объекты (людей, транспорт, зоны и т.д.), но и отслеживает сценарии их поведения, а также прогнозирует критичные для бизнеса показатели. При этом вся обрабатываемая системой информация хранится в защищённом «облаке» «КРОК».

2.5.6. Программное обеспечение *WINanalyze* для прослеживания и анализа движений (*motion tracking & analysis software*)

WINanalyze – это пакет программ компании *Mikromak* для отслеживания движения [12], обеспечивающий анализ движения в видео. *WINanalyze* может автоматически отслеживать практически неограниченное количество объектов в видеофайлах и представлять результаты различными способами (графически в координатной системе, диаграммой скоростей, ускорения и т. д.). Поддерживаются импорт и экспорт из большинства распространённых приложений.

WINanalyze стало первым приложением для автоматического анализа движения, способное отслеживать объекты без маркеров. Используя методы распознавания образов, во многих случаях некоторые части объектов могут отслеживаться по всей цифровой видеопоследовательности без какого-либо взаимодействия с человеком. Ныне *WINanalyze Tracker* широко используется для приложений анализа движения – таких, как анализ походки человека, исследование травм задней части тела, исследования по выявлению крэш-тестов (*crash test*), захвата видеороликов, *General Motion Capture* и т.п.

WINanalyze обеспечивает выполнение следующих задач:

- автоматическое прослеживание значительного числа объектов (*automatic tracking of unlimited number of objects*);
- ввод видеофайла (например, в формате *AVI, Raw* и т.п.);
- линейная и точная трёхмерная калибровка (*linear and precise 3D calibration*);
- вывод результатов анализа движения в виде отслеженных местоположений или траекторий объекта (*motion analysis outputs & object "trajectories"*);
- Вывод данных об углах и расстояниях (*angles and distances*);
- Оценка скоростей и ускорений движения (*first and second derivatives over time*);
- Определение центров масс объектов (*center of mass*).

2.5.7. Программно-аппаратные средства компании «Синезис»

Компания-резидент Парка высоких технологий Беларуси ООО «Синезис» разработала компактное видеоаналитическое устройство для интеллектуальной обработки видео в системах охранного наблюдения.

Как правило, универсальный кодер и видеоаналитика используются совместно, что позволяет воспользоваться преимуществами каждого из них в отдельности. При этом в целях снижения нагрузки на каналы связи, видеоаналитика должна быть задействована на стороне абонента. Также для определённых видов видеоаналитики – например, для распознавания лиц, необходим видеоанализ несжатого потока с целью обеспечить максимальную точность. По этим причинам «облачную» инфраструктуру невозможно экономически эффективно использовать для первичной обработки видео без соответствующего оборудования на стороне абонента.

Тем не менее, «облачную» инфраструктуру можно эффективно использовать для масштабирования системы видеонаблюдения:

- хранения видео и метаданных видеоаналитики;
- подключения новых объектов наблюдения (например, торговых точек);
- реализации новых функций анализа метаданных и поиска в архиве;
- обслуживания большого числа пользователей.

Естественно, что повышение точности видеоаналитики способствует снижению нагрузка на каналы связи и «облачное» хранилище. Поэтому, если показатели точности видеоаналитики известны, поставщик услуги и потребитель могут легко подсчитать экономическую выгоду от её использования.

Например, для охраны периметра большой гелиотермической установки используются 300 камер высокого разрешения (1,2 Мп). При нормальных погодных условиях суммарный поток видеоданных составляет 1,8 Гбит/с. При неблагоприятных условиях, т.е., при зашумлении сигнала (например, ночью) поток увеличивается почти вдвое – до 3,5 Гбит/с. Применение обычного детектора движения позволяет сократить объём видеоданных в среднем на 80% при отсутствии глобальных изменений освещённости и погодных условий сразу на всех камерах.

Видеоаналитическое устройство «Синезис» соответствует международному стандарту *ONVIF* и имеет международные сертификаты *i-LIDS*. Оно может быть интегрировано в действующую систему охранного видеонаблюдения без замены имеющегося оборудования (кабелей, камер, записывающих устройств, мониторов пульта служб безопасности).

Программно-аппаратные средства, поставляемые ООО «Синезис», позволяют:

- подсчитывать число посетителей, входящих и выходящих из магазина или отдела;
- определять количество людей и время их ожидания в очереди;
- осуществлять мониторинг активности кассира;
- классифицировать объекты по их цвету для разделения по типу «посетитель / персонал»;
- классифицировать объекты по их размеру для разделения по типу «взрослый / ребёнок».

2.5.8. Биометрия – новые горизонты развития банковских сервисов

Использование биометрических методов идентификации для самообслуживания клиентов ныне определённо стало одним из главных трендов в сфере банковских технологий. При этом решения по распознаванию образов наиболее органично сочетаются с задачами видеобезопасности, т. к., многие устройства самообслуживания уже оснащены видеокамерами. С учётом постоянного улучшения технических характеристик камер и общего развития биометрических технологий использование распознавания образов открывает новые возможности для финансовых институтов. Немаловажно, что соблюдение задаваемых сегодня стандартов через несколько лет, вероятнее всего, станет обязательным для любого успешного банка.

Именно поэтому в 2017 году *BS/2* и *VisionLabs*, один из лидеров рынка по внедрению технологии распознавания образов, объявили о стратегическом партнёрстве и создании линейки межбанковских сервисов идентификации. Сервисы будут строиться на базе комплексной системы видеомониторинга устройств самообслуживания *ATMeye.iQ* и платформы *LUNA*.

«В наши дни банки собирают огромное количество данных о своих клиентах, в том числе, фотографируют их при заключении договоров, оформлении кредитов и карт. Запечатлённые образы могут быть эффективно использованы для того, чтобы в дальнейшем определить добросовестных клиентов или мошенников, находящихся в «чёрном списке». Как только подозрительная личность подойдёт к устройству самообслуживания и попадёт в объектив стандартной портретной камеры банкомата, система *ATMeye.iQ* может отправить тревожное уведомление сотрудникам службы безопасности или запустить другой запрограммированный сценарий (отказ в обслуживании, захват банковской карты и

т.д.). Данная интеграция позволяет нам предлагать клиентам отличное решение для действенной комплексной видеобезопасности, ведь это именно то, что требует рынок банковских услуг в наши дни», - отмечает заместитель директора BS/2 Томас Аугуцявичюс.

2.6. Практические области применения видеоаналитики

Такие задачи, как защита головного офиса, отделений банка и круглосуточных банкоматов, выявление случаев мошенничества, наблюдение за подсчётом наличных, маркетинговый анализ и контроль эффективности рекламы, входят в список неотложных и повседневных для банков.

В сфере розничной торговли также существует большая потребность в системах безопасности. Их задача — с помощью видеонаблюдения создать на своих объектах «безопасные зоны» и вести мониторинг товарных запасов и иного имущества, а также бороться с воровством в торговых залах. За коммерческим сегментом следует рынок инфраструктурных объектов. Важный вклад в рост спроса на видеонаблюдение внесёт также финансовая сфера, где востребованы задачи тщательной охраны отделений банков и банкоматов. Новые возможности для интеграторов систем безопасности возникают и в сфере гостиничного бизнеса, где должный уровень безопасности постояльцев обеспечивается с помощью видеонаблюдения в коридорах и холлах отелей.

В разделе 3.2.1. описаны сценарии применения распознавания лиц для устройств самообслуживания в комплексе с системой *ATMeye.iQ*.

Ныне, в условиях острой конкуренции в сфере розничной торговли видеоаналитика приобретает особую значимость. При

этом важным фактором её применения является то, что для большинства актуальных задач предприятиям розничной торговли не требуется высокая точность результатов. В качестве примеров можно привести маркетинговый анализ предпочтений покупателей, включая оценку их количества, продолжительность осмотра продуктов, траектории и интенсивность движения клиентов по торговому залу.

Российская компания «Видеоинтеллект» специализируется на разработке алгоритмов безопасности для мест массового скопления людей. Она разработала программное обеспечение для распознавания поведения покупателей в офлайн-магазинах. Система позволяет распознавать готовность покупателя к покупке и его интерес к товару, а также заранее обезопасить себя от готовящейся кражи.

Зачастую в требованиях к системам видеоаналитики для обеспечения необходимого уровня безопасности указываются допустимые диапазоны вероятностей ложных срабатываний алгоритмов (*false alarm ratio*) от 1 до 5% процентов.

При этом поток в 100 тыс. человек в день и минимальная (1%) планка ложных срабатываний дают результат в 1 тыс. человек. Иными словами, это в среднем 125 человек в час – или примерно 2 человека в минуту.

На практике это означает, что служба контроля будет полностью парализована отслеживанием ложных сигналов уже в течение первых часов эксплуатации системы. В данном случае следует учитывать также психологический фактор. Сотрудник службы безопасности, принимающий большое количество ложных сигналов, не будет уже таким внимательным к реально происходящему важному событию. Для полноценной работы систем в таких условиях необходимы значения вероятностей на один или (что лучше) на несколько порядков меньше.

Система «Видеоинтеллект» анализирует сцены и достигает параметров: 0,3-0,6 ложных срабатываний на видеокамеру в сутки, что составляет тысячные доли процентов ложных срабатываний.

Использование нейронных сетей в видеонаблюдении открывает огромные перспективы и широкие области применения этой технологии – от розничной торговли до решений «умного города». Для сферы безопасности — это серьёзный скачок в развитии ситуационной аналитики, и переход от предположений, основанных на математическом анализе геометрии и цветовых характеристик набора пикселей, к распознаванию образов.

ATMeye.iQ

Решение для видеонаблюдения и предотвращения мошенничества

ATMeye .iQ
.iQ Family Product

ATMeye.iQ – комплексное решение для повышения уровня безопасности устройств самообслуживания. Оно включает в себя систему видеонаблюдения с функциональностью распознавания лица, а также датчики, реагирующие на любые противоправные действия в отношении терминалов.

Глава 3. Программные решения для поддержки современных систем видеонаблюдения

«Я понимаю, КАК; не понимаю зачем…»

Дж. Оруэлл, «1984»

Мошенники, которые разрабатывают множество нацеленных на банкоматы атак, в зависимости от своих мотивов ориентируются на различные элементы оборудования.

В отличие от атак на физические элементы банкоматов, *логические атаки* нацелены на сразу все банкоматы в сети. Это означает, что они подвергаются угрозам на основе программного обеспечения – аналогичным тем, с которыми сталкиваются другие сетевые ПК. Потенциальный размер выигрыша для злоумышленника здесь намного выше.

Демонстрация логических атак, нацеленных на банкоматы, была проведена ещё в 2010 году на конференции *Black Hat* в Лас-Вегасе. С тех пор любые мошеннические действия, в результате которых перепрограммированный банкомат выдавал злоумышленникам все содержимое своих кассет, стали называть «*джекпоттингом*» (j*ackpotting*).

К числу наиболее распространены следующие виды логических атак следует отнести:

- «*Джекпоттинг»* – вредоносное программное обеспечение заставляет машину выдавать деньги без создания транзакции. Известные методы включают прямую установку вредоносного приложения на жёсткий диск ПК банкомата, с помощью нежелательной перезагрузки с компакт-диска или флэш-накопителя (*USB*), или сетевое действие;

- «*Чёрный ящик» (Black Box*) – внешний компьютер подключён к банкомату и приказывает ему выдать наличные;
- «*Хост-спуфинг*» (*Host Spoofing / Man-in-the-Middle*) – управление ответами сервера или запись важных данных внутри сети.

По мере увеличения пропускной способности банкоматов также растёт вероятность атаки на них. По данным аналитической компании FICO, лишь в США в 2016 году число случаев компрометации банкоматов и торговых устройств выросло на 30%.

Так, в 2016 году отмечено 25 588 атак на банкоматы, что на 26% больше, чем в 2015 году. Это проблема не только одних США: 10 европейских стран также сообщили о логических атаках на банкоматы в 2016 году. В том же году количество платёжных карт, скомпрометированных в США, выросло на 70% [17].

Рост числа технологических атак в последние несколько лет объясняется тем, что мошенники разрабатывают новые способы вторжения во внутренние процессы, когда:

- персонал или посторонние участники превышают свои уровни разрешений;
- недобросовестные инсайдеры предоставляют доступ злоумышленникам посредством фишинга или социальной инженерии;
- персонал, работающий с наличными средствами, пользуется слабыми местами процесса, похищая деньги из кассеты или на необработанной фазе во время перемещения наличных.

Поэтому финансовые учреждения должны создавать слой защиты на уровне безопасности своей среды АТМ от всех видов мошенничества.

В своём первом отчете по борьбе с мошенничеством на 2018 год Европейская ассоциация безопасных транзакций (*European*

Association for Secure Transactions; EAST) оценила текущее положение на основе последних данных о преступности в 18 странах, входящих в «Единую платёжную зону евро» (*Single Euro Payments Area; SEPA*), и 4 странах, не входящих в SEPA [19].

С целью снижения рисков от этих типов атак Europol, поддержанный EAST EGAF, опубликовал «Руководство и рекомендации относительно логических атак на банкоматы» *(Guidance and recommendations regarding logical attacks on ATMs).*

3.1. Краткий обзор средств информационной безопасности от ведущих производителей, сопутствующих современному видеонаблюдению

Швейцарская компания-поставщик решений для обеспечения безопасности банкоматов *TMD Security GmbH* в партнёрстве с британским провайдером программного обеспечения для управления и мониторинга банкоматов, устройств внесения наличных денег и их переработки *S3 Technologies Ltd.* разработала программное обеспечение *TMS ATM*, предназначенное для защиты от логических атак с использованием вредоносных программ или устройств «чёрного ящика», применяемых для «джекпоттинга» банкоматов.

TMS ATM обнаруживает несанкционированные изменения программного обеспечения или оборудования с управлением профилями; блокирует использование неутвержденных запоминающих устройств *USB*; контролирует доступ *Windows* к банкоматам и помогает оператору безопасно управлять паролями *BIOS* с управлением доступом.

Diebold Nixdorf

BS/2
Penki kontinentai group

Компания BS/2 более 25 лет сотрудничает с мировым лидером в сфере банковских технологий и крупнейшим производителем банкоматов – концерном Diebold Nixdorf, внедряя передовые технологические решения для банков и сферы розничной торговли по всему миру.

3.1.1. Решения *Diebold Nixdorf*

Программный комплекс *Vynamic Security* (известный ранее как *Terminal Security Suite*) от *Diebold Nixdorf* предлагает мультивендорное программное обеспечение для защиты от логических и иных атак. Состоящий из четырёх модулей (*Access Protection, Intrusion Protection, Hard Disk Encryption* и *Fraud Protection*) программный комплекс обеспечивает защиту банкоматов и других устройств в режиме реального времени, реализуя принцип тотального ограничения на запуск любых процессов и действий.

Декларируемый принцип работы ПО состоит в запуске одних лишь разрешённых и многократно проверенных процессов – и никаких других. Этот принцип «белых списков» (*whitelisting*) призван защитить компьютер устройства самообслуживания от несанкционированного использования внешних устройств (флэш-карт, жёстких дисков и других потенциальных носителей вредоносного ПО).

Кроме того, *Vynamic Security* устанавливает набор правил на основе технологии «песочницы» (*sandboxing*), когда имеющему конкретное назначение ПО предоставляется строго заданный набор ресурсов и регламентированный доступ на компьютере.

Vynamic Security также следит за отсутствием несанкционированных изменений в уникальной созданной «экосистеме» банкомата с конкретным набором технического оборудования и приложений. При попытке замены жёсткого диска извлеченный носитель, содержащий конфиденциальную информацию, приходит в негодность (за что отвечает модуль *Hard Disk Encryption)*, а на самом банкомате может быть запущен один из сценариев тревоги.

Отдельно стоит отметить модуль *Fraud Detection* – который, с помощью технологий *Big Data* и машинного обучения, позволяет отслеживать отклонения в стандартных сценариях поведения программ, процессов и пользователей.

Как уже отмечалось в разделе 2.3, при выявлении отклонений от шаблонов поведения пользователей могут применяться заранее предусмотренныемерыбезопасности.

Благодаря запуску решения *Diebold Nixdorf AllConnect Services* финансовые учреждения и предприятия розничной торговли получили возможности и технологии, необходимые для того, чтобы каналы физического распространения стали равноценными их цифровым аналогам по гибкости, интегрированности, эффективности.

С этой целью *Diebold Nixdorf AllConnect Services* использует инфраструктуру *IoT* как основу для всех конечных точек обслуживания, которые интуитивно анализируют данные для прогнозирования трендовых результатов и процесса принятия решений.

С помощью нового мультивендорного ПО для банкоматов *ProFlex4* банки могут модернизировать и оптимизировать пользовательские интерфейсы своих банкоматов с использованием новейших веб-технологий.

Кроме того, новые концепции сервиса – такие, как снятие наличных денег с помощью смартфона вместо банковской карты, или персональные пользовательские интерфейсы – легко реализуются с *ProFlex4.*

Таким образом, банки могут самостоятельно добавлять новые предложения на своих банкоматах или же создавать индивидуальные пользовательские интерфейсы, или они могут обратиться в службу ИТ и профессиональных услуг Diebold Nixdorf для его развития и внедрения.

Следует отметить, что платформа *ATMeye.iQ* уже интегрирована с *ProFlex4.*

3.1.2. Решения Ingenico Group

Ingenico Group является одним из немногих производителей специализированного терминального оборудования в местах продажи (*point of sale; POS*), успешно реализующий технологии массовой биометрической идентификации.

Так, компания реализовала ряд проектов, ориентированных на привлечение к банковскому обслуживанию не охваченных ранее слоёв населения с помощью биометрии.

Эти проекты призваны облегчить переход продавцов на многоканальные продажи через широкий спектр смарт-терминалов, платёжных услуг и мобильных решений, охватывающих Интернет-магазины, онлайн- и мобильные каналы в глобальном масштабе.

Одной из последних разработок *Ingenico Group* является *Axium* – открытая платформа *Android POS* для цифровизации коммерческой торговли в стационарных магазинах, разработанная с учётом потребностей покупателей. Она предоставляет доступ к полной «облачной» экосистеме для торговли, основанной на открытых операционных системах *Android* и *Ingenico Telium Tetra*.

Визуально новое устройство *Axium* напоминает планшетный компьютер с кассовым аппаратом. При этом оно умеет не только проводить полное кассовое обслуживание, но и поддерживать любые приложения для *Android*

3.1.3. Решения *Gemalto*

Предприятия, стремящиеся расширить масштабы развёртывания облачных приложений по организациям, сталкиваются с препятствиями для эффективного управления «облачными» идентификаторами и «облачным» доступом, обеспечивая при этом удобство пользователя и соблюдение нормативных требований.

Предлагая полностью автоматизированную проверку подлинности на основе «облачных» вычислений и обширное управление жизненным циклом, платформы управления аутентификацией компании *Gemalto* предназначены для упрощения развёртывания в сложных средах, снижения административных накладных расходов и создания прочной основы для масштабирования как в «облачных», так и локальных средах инфраструктуры открытых ключей (*Public Key Infrastructure; PKI*).

Основываясь на своём сервисе мультифакторной аутентификации, *Gemalto* предлагает *SafeNet Trusted Access (Identity-as-a-Service)* – интуитивно понятную службу, упрощающую управление облачным доступом на основе единого входа и на основе сценариев. *SafeNet Trusted Access* сочетает в себе удобство «облачного» единого входа (*single sign-on; SSO*) с расширенной безопасностью доступа и упрощает управление «облачными» идентификационными данными, устраняя проблемы с безопасностью для ИТ-персонала и пользователей, предоставляя единое окно событий доступа по своему «облачному» пространству.

Решение биометрической аутентификации *Gemalto Mobile Protector* поддерживает распознавание как отпечатков пальцев человека, так и его лица с помощью простых *API*-интерфейсов для разработчиков, которые внедряют эти функциональности в специализированные приложения [18]. При этом *Gemalto Mobile Protector* обеспечивает безопасное использование

биометрических данных, исключая необходимость их хранения в дата-центре или на серверах. Указанные данные остаются в мобильном телефоне пользователя, гарантируя безопасность.

Gemalto предоставляет оптимизированный пользовательский интерфейс «под ключ» – в связи с чем банки смогут запускать биометрический проект и оценить, как интегрировать его в рамках существующего пользовательского интерфейса.

В рамках универсального комплекта цифрового банковского обслуживания *Gemalto Mobile Protector* удачно вписывается в жизненный цикл безопасности банка. Он может сопровождаться выбором дополнительных продуктов – таких, как *Gemalto Confirm Authentication Server* (*CAS*).

3.1.4. Решения SSC

Основанная в 2004 году компания *Skaitmeninio sertifikavimo centras* (*SSC*), и входящая ныне в группу предприятий *Penki kontinentai*, первой в Литве начала предоставлять услуги по созданию квалифицированных сертификатов электронной цифровой подписи (*ЭЦП*) – и других связанных с ними услуг.

Компания оказывает широкий спектр услуг на базе технологии *PKI* и имеет официальную государственную аккредитацию для выдачи квалифицированных сертификатов *ЭЦП* на европейском рынке. Квалифицированные сертификаты сегодня выдаются гражданам 21 стран мира.

Кроме того, *SSC* разрабатывает ПО для электронной подписи, оказывает услуги временной метки (*timestamp*), разрабатывает и внедряет систему единой федеративной аутентификации, не зависящей от используемых криптопровайдерами алгоритмов, и оказывает другие услуги на базе технологии *PKI*.

Аутентификация содержания документа выявляет, изменился ли он с момента его подписания. В свою очередь, аутентификация людей устанавливает, действительно ли подписавший документ в формате PDF человек является тем лицом, за которого он себя выдаёт.

Для финансового и государственного секторов компания создала линейку программных продуктов *Justa* для электронной подписи, включающую:

- *Justa WEB ID* (федеративная аутентификация);
- *Justa PDF Sign* (подписание PDF);
- *Justa Smart Forms* («умные» PDF формы).

Так, *Justa PDF Sign* — это программное обеспечение для подписания PDF-файлов, которое может быть распространено как услуга, а специальные дистрибутивы могут быть интегрированы в любую новую или существующую ИТ-систему. При этом *Justa PDF Sign* является единственным ПО для подписи PDF, которое может быть распространено как услуга и персонализировано для каждого сертификата или пакета сертификатов для корпоративных пользователей.

Подписи, созданные при помощи *Justa PDF*, могут быть проверены с использованием стандартного бесплатного *Adobe Reader 7.0+*. Подписанные документы PDF обеспечивают целостность данных документа – и позволяют определить, кто подписал документ. Проверка — это сертификат, используемый для подписи, который остаётся действительным и не отменяется.

PDF Sign доступен в нескольких языковых версиях, включая английскую, русскую, французскую, литовскую, голландскую и другие.

Компания *SSC* является участницей проекта *eTen* консорциума *Billing for Rent*, финансируемого Европейской Комиссией; наряду с такими компаниями, как *Google, Apple, Microsoft, Symantec* и др. является членом международного форума

CA/Browser; ежегодно участвует в одном из наиболее важных мероприятий на тему информационной безопасности – конференции *RSA* (США).

Соответствие услуг *SSC* международным стандартам подтверждён независимой компанией по аудиту *TÜV Informationstechnik GmbH* (*TÜViT*).

3.2. Распознавание лица как практический метод аутентификации и обеспечения безопасности в банковском секторе

Применение и распознавание биометрических данных – одно из наиболее активно развивающихся технологических направлений. В банковской сфере, где проблема безопасной и надёжной авторизации клиентов наиболее актуальна, этот «биометрический» тренд, в особенности, технология распознавания по лицу стал весьма востребованным.

Во многих финансовых организациях уже используются следующие биометрические методы для идентификации, авторизации и верификации личности:

- Распознавание по лицу (*facial recognition*) – по цифровому представлению лица человека проводится его идентификация, когда изображение на входе в систему (фотоснимок или видеопоток) сравнивается с хранящимся в базе данных цифровым представлением лица этого же человека. Для работы этого метода необходимо использовать устройство фото- или видеосъёмки.
- Распознавание по рисунку венозных капилляров на ладони или пальцах (*palm / finger vein recognition*) – это преобразование образцов рисунка капилляров в цифровое представление для последующего сравнения

- с существующей базой данных. Для работы по этому методу необходим специализированный сканер.
- Распознавание по отпечатку пальца (*fingerprint recognition*) – с помощью дактилоскопического метода, основанного на уникальности рисунка на пальце, проводится идентификация личности. Для работы по этому методу также потребуется специализированный сканер.
- Распознавание голоса (*voice recognition*) – это преобразование голосового сигнала в цифровое представление для дальнейшего установления соответствия в существующей базе данных. Для работы необходимо устройство записи голоса.
- Распознавание по радужной оболочке глаза (*iris recognition*) – это преобразование изображения радужной оболочки глаза в цифровое представление для дальнейшего нахождения соответствия в существующей базе образов. Для работы потребуется специализированное устройство съёмки изображения радужной оболочки глаза.

Благодаря функционалу распознавания по лицу можно предоставить клиентам дополнительные меры безопасности при выполнении операций, с одной стороны, и автоматизировать ряд процессов – с другой.

Сбор и обработка биометрических данных являются важнейшим этапом развития интеллектуальных банковских услуг.

Перечисленные технологии могут использоваться как в отношении сотрудников банка для организации защищённого доступа к их рабочим местам (двухфакторная аутентификация для доступа к внутренним системам банка), так и для банковских процессов, обращённых к клиентам. Среди таких процессов следует выделить:

- принятие решения о предоставлении кредита (оценка платёжеспособности заёмщика) в баллах;
- аутентификацию в системе обслуживания клиентов;
- полуавтоматическое заполнение заявок данными из удостоверения личности;
- дополнительную аутентификацию при регистрации в мобильном приложении;
- идентификацию мошеннических действий и поиск мошенников, включая межбанковский обмен биометрическими данными лиц, занесенных в «чёрные списки».

Большинство технологий могут использоваться также для процессов, связанных с работой устройств самообслуживания (банкоматов, киосков и т.д.). С точки зрения развёртывания решения наиболее простым является внедрение системы распознавания лиц, не требующей установки специализированного оборудования на устройство самообслуживания, и для работы, которой достаточно уже установленной фронтальной камеры системы видеонаблюдения. При этом система распознавания лиц может быть интегрирована в систему видеомониторинга, предоставляя комплексную систему обеспечения безопасности как самого устройства самообслуживания, так и проводимых на нём транзакций.

Ниже рассмотрены возможные сценарии такого использования системы распознавания лиц.

3.2.1. Сценарии применения распознавания лиц для устройств самообслуживания в комплексе с системой *ATMeye.iQ*

На протяжении ряда лет компания-разработчик программных решений для безопасности устройств самообслуживания *BS/2*, создала такие продукты, как *ATMeye.iQ* (решения для повышения безопасности устройств самообслуживания), *Brancheye.iQ* (расширение до *IoT*), *CashManagement.iQ* (для авторизации инкассаторов), ServiceDesk.iQ (для авторизации сервисного персонала), *SmartSafe.iQ* (видеоконтроль за действиями кассира и для работы в режиме самообслуживания).

Решение *ATMeye.iQ*, которому посвящена гл. 4, предусматривает дополнительную опцию по распознаванию лица человека, которая обычно не требует установки специализированного оборудования на устройстве самообслуживания. Для полноценной работы с ним достаточно уже имеющейся фронтальной камеры системы видеонаблюдения.

Система полностью совместима с устройствами самообслуживания от большинства мировых производителей (*Diebold Nixdorf, NCR, Hyosung* и других).

С другой стороны, сбор биометрических данных позволяет создать в системе «белый список» для инженеров, обслуживающих устройства, и сотрудников инкассаторских служб. В случае несанкционированного доступа к устройству оповещение о событии вместе с фото- и видеоматериалами высылаются сотрудникам службы безопасности для своевременного реагирования.

Кроме того, система распознавания лиц способна определять пол и примерный возраст людей. Таким образом, данная функциональность может использоваться для показа адресной

рекламы конкретной категории клиентов. Эта функция может быть реализована не только в устройствах самообслуживания, но и практически в любом месте, где клиенты останавливаются для проведения каких-либо действий (заполнения бланков, договоров, получения билета и т.д.).

Двухфакторная авторизация на устройствах самообслуживания может быть использована для предоставления дополнительного уровня безопасности при проведении операций с банковскими картами, а также для предотвращения попыток использовать карту посторонним лицом.

В рамках данного сценария при выдаче карты обязательным действием должна быть фотосъёмка владельца карты по предъявлении им удостоверения личности и его идентификации работником банка. Фотосъёмка должна проводиться в хорошо освещённом помещении и камерой с высокой разрешающей способностью (*HD*).

В дальнейшем при проведении банковских операций на устройствах самообслуживания после ввода PIN-кода камера осуществляет фиксацию лица клиента, проводящего транзакцию; затем производятся выбор наилучшего кадра из видеопотока, предоставляемого системой *ATMeye.iQ,* и сравнение снимка этого человека, с оригиналом, хранящимся в базе данных. При этом уровень совпадения должен быть задан в пределах 90-95%.

Важно подчеркнуть, что, чем выше уровень совпадения, тем меньше риск неправомерного использования банковской карты. При этом привязка лица проводится по номеру карты.

Если система распознавания лиц подтверждает совпадение с фотографией из базы данных, то этому человеку предоставляется доступ к последующим (после ввода PIN-кода) окнам на экране банкомата. В противном случае карточка удерживается с выдачей соответствующего сообщения на экран банкомата и указанием номера телефона, по которому можно

получить консультацию. Если произошла ошибка, то по предъявлению удостоверения личности в отделении банка карта клиенту будет возвращена.

Занесение в «*чёрный список*» для предотвращения мошеннических действий. В «чёрный список» заносятся лица, ранее замеченные в попытках различных мошеннических действий, и чьи фотографии были собраны с помощью системы видеомониторинга устройств самообслуживания или прилегающей территории.

Предотвращение мошеннических действий при использовании устройств самообслуживания может проводиться совместно с двухфакторной авторизацией, или же без неё. Лица, которые используют чужие банковские карты, могут быть занесены в «чёрный список». Фиксация лица, выбор наилучшего кадра и запись его в базу данных проводится из видеопотока, записываемого системой *ATMeye.iQ*.

В дальнейшем по событию ввода PIN-кода проводится фиксация лица клиента, выбор наилучшего кадра – и осуществляется поиск совпадений в «чёрном списке». При этом уровень совпадения должен быть задан в пределах 96 - 99%, с тем, чтобы избежать возможной ошибки.

При обнаружении совпадения система *ATMeye.iQ* инициирует тревожный сигнал и оповещает сотрудников службы безопасности для оперативного реагирования. Возможна разработка дополнительного сценария, позволяющего как можно дольше задержать подозрительного человека перед банкоматом.

«*Белый список*» для доступа к обслуживанию устройств самообслуживания. «Белый список» определяет сотрудников, которым предоставлен доступ к тому или иному устройству самообслуживания. Сервисные инженеры и работники инкассаторской службы, у которых есть соответствующий допуск на работу с устройствами самообслуживания, заносятся

в этот список службой персонала, с одновременным сохранением их фотография в базе данных.

При формировании бригад на инкассацию банкоматов или при получении инженером наряда на работу с определёнными устройствами самообслуживания эти лица заносятся непосредственно в «белый список», разрешающий им работу с конкретными устройствами самообслуживания. Для реализации данного функционала необходима интеграция с системой *Service Desk.iQ* и *Cash Management.iQ* (см. гл. 4).

Для распознавания лица обслуживающего персонала необходимо около *SOP* панели разместить подключенную к системе *ATMeye.iQ* видеокамеру, которая будет фиксировать всех людей, которые производят работы внутри банкомата. Видеокамера должна передавать в систему *ATMeye.iQ* событие по срабатывании сенсора открытия дверцы банкомата. По тому же событию должна начаться запись видео с внутренней камеры банкомата, с последующим фиксированием лица, выбором наилучшего кадра и поиском совпадения в «белом списке» применительно к данному устройству самообслуживания. Уровень совпадения должен быть выставлен в пределах 80-85% для того, чтобы избежать излишние проверки при не распознавании лица.

В случае, если лицо не найдено в «белом списке» банкомата, сотрудники службы безопасности оповещаются через систему *ATMeye.iQ* для оперативного реагирования на создавшуюся ситуацию.

Распознавание пола, возраста и показ адресной рекламы. Помимо функции сравнения с эталоном, хранящемся в базе данных, система распознавания лиц способна определять пол и приблизительный возраст людей. Таким образом, появляется возможность использования данной функциональности для показа целевой аудитории адресной рекламы.

Система распознавания пола и возраста начинает свою работу при фиксации лица. Из видеоряда продолжительностью в 10-20 сек выбирается наилучший кадр и производится распознавание. Если распознавания не произошло с достаточной долей вероятности, система продолжает показ предыдущей рекламы. В случае успешного распознавания пола и возраста выводится рекламный ролик, заранее подготовленный для данной целевой аудитории. Набор рекламных видеосюжетов хранится на устройстве самообслуживания или в системе управления рекламным дисплеем.

Время отображения каждого рекламного ролика определяется пользователем системы. При этом должна быть представлена возможность конфигурировать рекламные сюжеты для каждого дисплея и устройства самообслуживания.

Глава 4. Семейство программных продуктов *«.iQ»*

«Свобода – это возможность сказать, что дважды два – четыре. Если позволено это, то остальное отсюда следует»

Дж. Оруэлл, «1984»

В ноябре 2015 года *Forrester Consulting* по поручению компании *Diebold Nixdorf* провёл всесторонний анализ проблем, с которыми сталкиваются розничные банки в управлении безопасностью своих парков банкоматов. В результате опроса руководителей бизнеса и ИТ во всём мире было подтверждено, что банки лишь выиграют от партнерства с внешним провайдером в управлении безопасностью своего парка банкоматов.

Результаты показали, что среднее финансовое учреждение имеет в своём распоряжении от 100 до 499 банкоматов на региональном уровне – что представляет значительный риск проникновения потенциальных угроз, защита от которых должна быть надёжно обеспечена.

Ил. 3. Семейство продуктов «.iQ»

4.1. *ATMeye.iQ* – платформа безопасности и видеомониторинга устройств самообслуживания

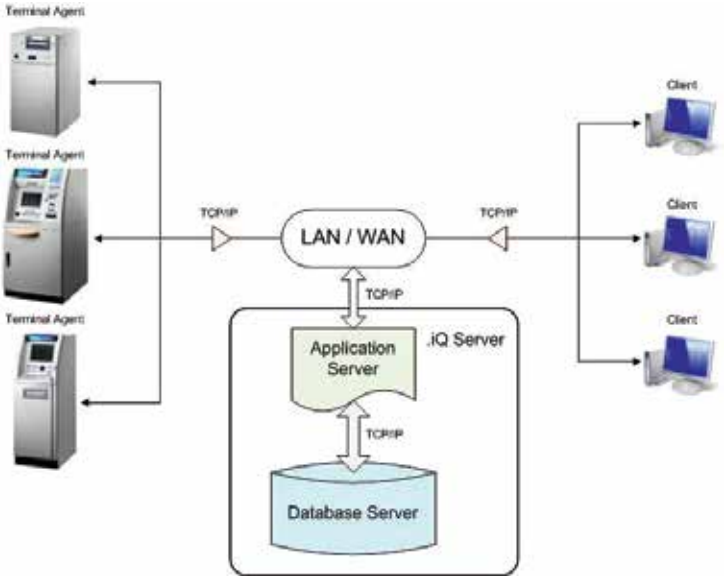
ATMeye.iQ — программно-аппаратное решение для повышения уровня безопасности устройств самообслуживания в режиме реального времени и обеспечения своевременной реакции на неправомерные действия. Оно является частью семейства продуктов *«.iQ»* для управления и мониторинга бизнес-процессов, специально разработанного для финансовой индустрии.

Рост сетей банкоматов является серьёзным испытанием для банков. Этот тренд требует от финансовых организаций дополнительных затрат на увеличение персонала и заметно усложняет рабочие процессы, связанные с техническим обеспечением работы устройств. Именно поэтому очень

актуальна предоставляемая *ATMeye.iQ* возможность защитить до 14 000 терминалов в рамках одной сети [15].

Ил. 4. Схема решения ATMeye.iQ.

Платформа *ATMeye.iQ*, появившаяся на рынке ещё в 2001 году, включает в себя систему видеонаблюдения, а также датчики, реагирующие на любые противоправные действия в отношении терминалов.



Ил. 5. Концептуальная схема платформы ATMeye.iQ и её составляющие модули.

Платформа предназначена для организаций, использующих сети терминальных устройств самообслуживания, и заинтересованных в повышении уровня безопасности обслуживания клиентов и устройств самообслуживания.

Ядро системы *ATMeye.iQ* функционирует на основе архитектуры клиент-сервера, система использует единую централизованную базу данных, создавая возможность доступа к необходимым данным для различных групп пользователей, обеспечивая целостность и непротиворечивость информации. Оно состоит из следующих основных компонентов: *USM.iQ* (модуль управления пользователями и безопасностью), *ADM.iQ* (модуль управления ресурсами) и *DTC.iQ* (модуль сбора данных).

Модуль *DTC.iQ* предназначен для интеграции системы *«.iQ»* с внешними системами. Он поставляет как оперативную

информацию о событиях во внешних системах (вставление карточки, выдача наличных на банкомате, получение нового запроса на обслуживание и т.п. события), так и информацию об изменениях в конфигурациях внешних систем (введение нового устройства, изменение адреса установки устройства, изменение статуса внешней компании и т.п.).

Для доставки информации из внешних систем модуль *DTC.iQ* использует конфигурируемых агентов, которые гибко адаптируются к условиям новых задач. Вся поставляемая агентами информация сохраняется в базе данных как в исходном, так и в пригодном для использования системой *«.iQ»* виде. Информация от внешних устройств проходит фильтрацию, и на вход *«.iQ»* поступает только рабочая информация.

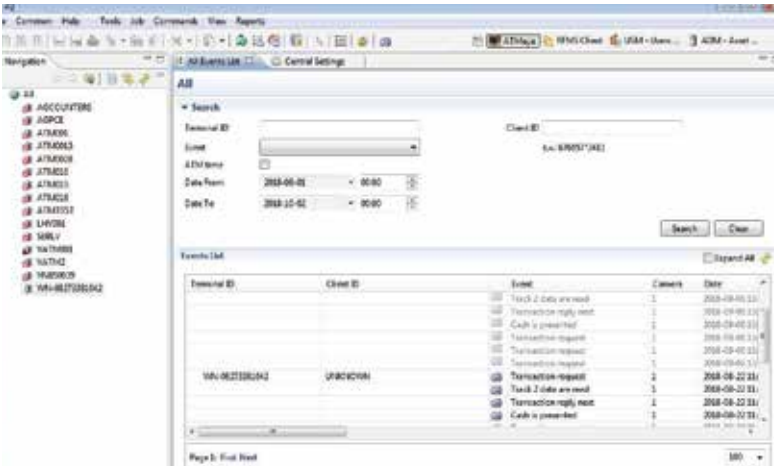
При работе в системе используется криптографический протокол *TLS 1.2*, который обеспечивает установление безопасного соединения между клиентом и сервером в соответствии с сертификатом *PA-DSS*.

В 2017 году был осуществлён глобальный переход на версию *ATMeye.iQ 2.0*, в которой впервые реализована возможность дистрибуции программных лицензий для устройств самообслуживания напрямую с сервера. Таким образом, клиентам и партнёрам компании предоставляется инструмент для простого управления действующими лицензиями ПО, улучшая их взаимодействие.

Отметим, что с *ATMeye.iQ* интегрирован *ProView* — программный комплекс компании *Diebold Nixdorf*, предназначенный для мониторинга и управления сетями банковских устройств самообслуживания, дистанционного администрирования, диагностики и генерации отчётов.

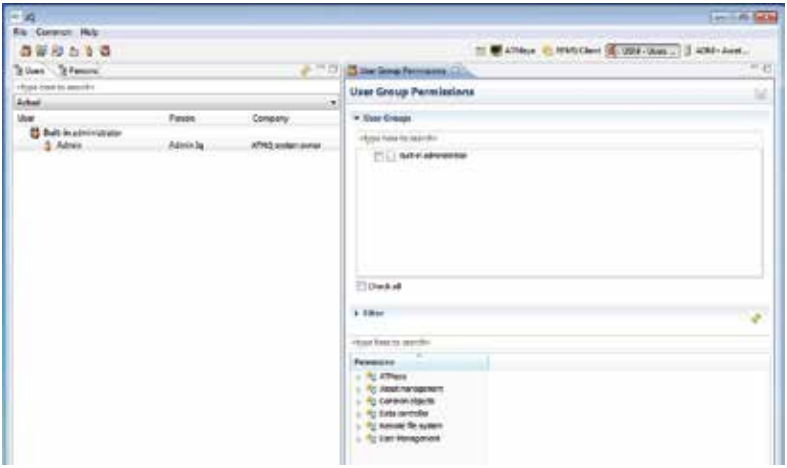
Для связи с сервером разработана программа *«.iQ» Client* (рабочее место оператора / администратора), которая после установки на компьютере клиента предоставляет ряд

интерфейсов управления. Эти интерфейсы (под названием *Perspectives*) предназначены пользователям *«.iQ»* системы с различными ролями и разрешениями доступа. Указанная программа содержит несколько модулей. В их числе – базовые (*Basic*) и дополнительные клиентские модули (*Client*), которые выбираются самим пользователем, согласо приобретённым ими лицензиями.



Ил. 6. Главный экран для мониторинга устройств и транзакций программа. «.iQ» Client.

На главном экране приложения *«.iQ»* Client (ил. 6) показан центральный вход в систему: на этом экране слева в дереве устройств отображаются имеющиеся устройства (банкоматы и т.п.); если дерево будет разделено на группы устройств, то будут отображаться только те из них, которые разрешены администратором системы. Модули системы указываются при переходе в модули *USM*, *ADM* и *RFM* во время установки программы. Базовых модулей два: *Users («Пользователи»)* и *Assets («Активы»)*.



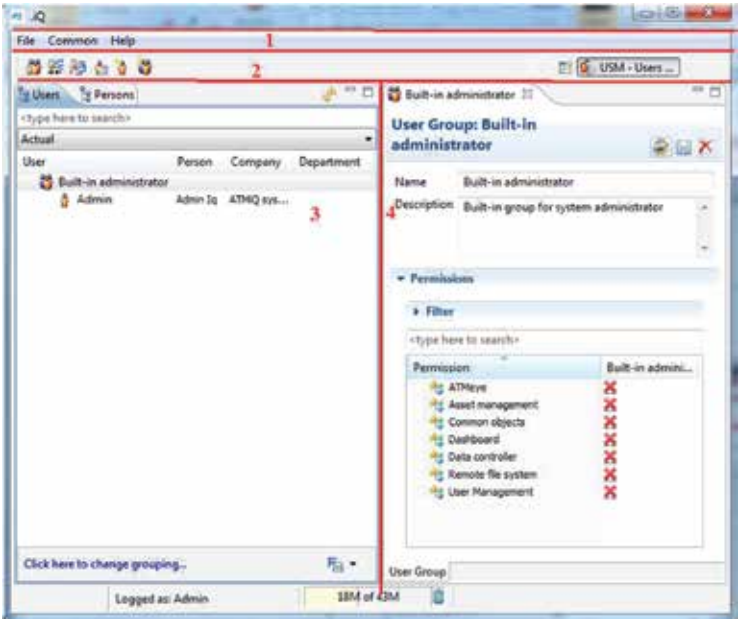
Ил. 7. Главный экран для перспективы USM.iQ

Модуль *USM (Users and Security Management)* для управления пользователями и их правами доступа. В этом модуле перспектива «*Users*» предоставляет интерфейс для управления пользователями системы *«.iQ»*. В перечень общих функциональностей этой перспективы входят:

- создание, удаление, выключение пользователей;
- ввод и редактирование необходимых атрибутов информации о пользователе;
- управление правами доступа к модулям и компонентам системы *«.iQ»*.

Панель разрешений для пользовательской группы (*User Group Permissions*) состоит из двух частей:

- список пользовательских групп
- список объектов (формы, модули, функции), к которым разрешён доступ.

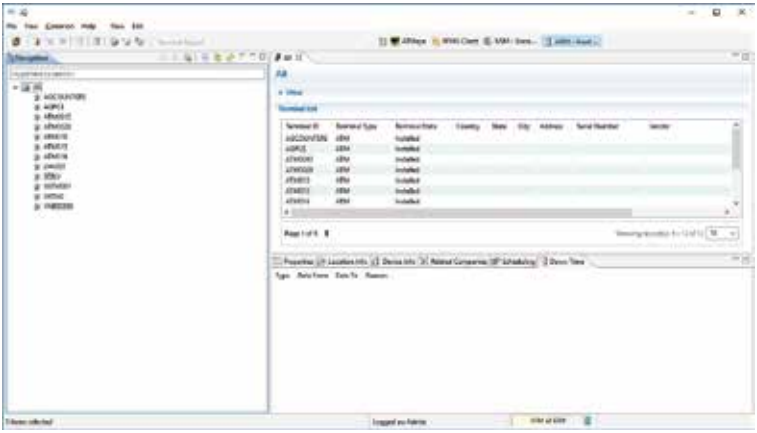


Ил. 8. Пользовательский интерфейс модуля USM.iQ.

Помимо создания новых групп пользователей и редактирования их свойств имеется возможность клонирования конкретной пользовательской группы. Это означает создание идентичной группы пользователей (но под другим именем) с теми же правами доступа, что и выбранная группа пользователей.

В системе фиксируются все действия пользователей; при необходимости можно просмотреть историю действий пользователя по заданным критериям поиска (имени пользователя, событию, периоду времени), генерации отчётов и т.д.

Модуль *ADM* (*Asset Device Management*) для управление активами предназначен для ввода устройств (банкоматы, киоски, *POS*-терминалы и т.п.), в систему. В систему вводится не только кодовое название оборудования, но и адрес, где это устройство установлено, его комплектующие и т.д.



Ил. 9. Главный экран для перспективы ADM.iQ

Перечень его функциональных особенностей включает:

- создание, удаление, восстановление, клонирование терминального устройства;
- ввод и редактирование атрибутов информации о терминальном устройстве;
- иерархическая группировка и выбор устройств;
- управление правами доступа к устройству для пользователей и групп пользователей;
- создание, редактирование, удаление сети, просмотр списка устройств.

Кроме того, можно просмотреть и редактировать список периодов, добавления и удаления неисправного состояния терминала, и т.д.

Модуль *RFM* (*Remote File Management*) для удалённого управления файлами обеспечивает передачу файлов между удалённым устройством самообслуживания и рабочим местом оператора по защищённому каналу связи.

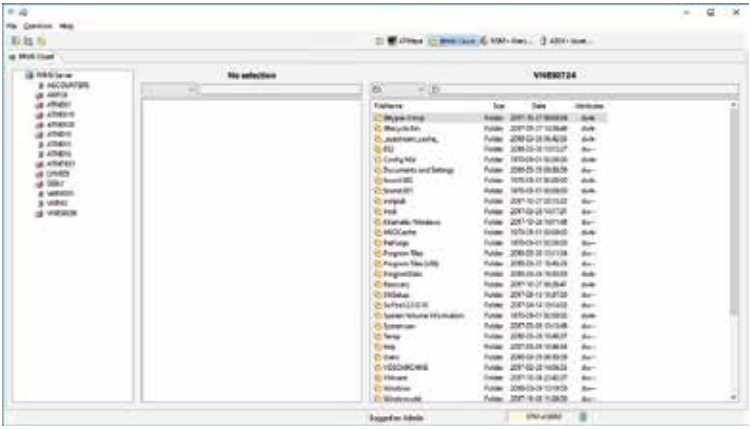
Система *RFM.iQ* включает:

- терминальный модуль *RFM.iQ*, который устанавливается на каждом устройстве;

- серверный модуль *RFM.iQ* с функциями управления правами пользователя *User Security Manager* и устройствами *Asset Device Management*.
- клиентский модуль *«.iQ» Client.*

Локальная панель системы поделена на 3 части:

- дерево устройств;
- окно файловой системы для выбора диска на выбранном устройстве;
- окно файловой системы, где отображаются файлы с компьютера, на котором запущен клиент *«.iQ»*.



Ил. 10. Главный экран для перспективы RFM.iQ.

Благодаря технологии *RFM* финансовые учреждения могут более эффективно организовать обмен данными между устройствами самообслуживания, оптимизировать работу сервисных служб и сокращать расходы. После активации устройства в системе все задачи по обмену данными выполняются удалённо по заранее заданному графику. При этом передавать данные можно как на конкретное удалённое устройство самообслуживания, так и на всю рабочую сеть в целом.

Область применения системы *RFM.iQ* включает банкоматы, электронные сейфы, информационные и платёжные терминалы, а также компьютеризированные рабочие места.

Решение *RFM.iQ* поставляется в качестве отдельного продукта или в комплекте с системой *ATMeye.iQ*.

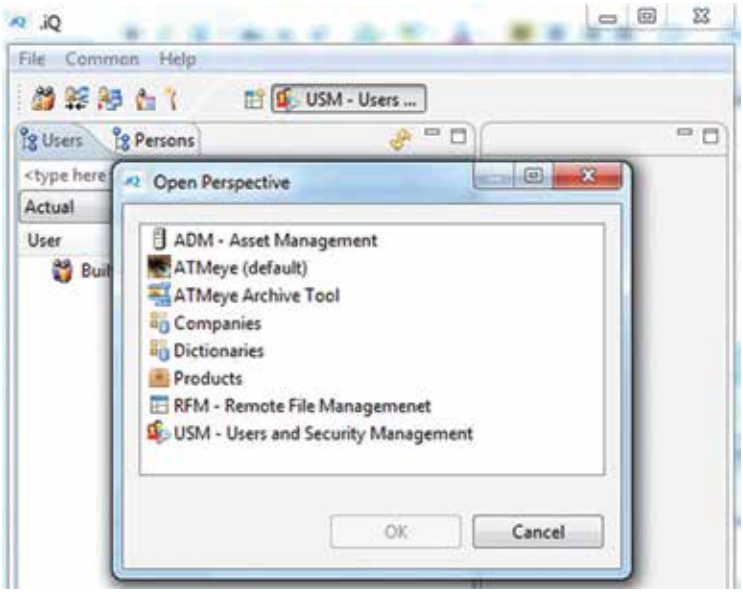
В числе основных функций модуля – удалённый поиск документов, передача файлов с удалённого терминала в базу данных или местную файловую систему, планирование задач (по числам, дням недели, папкам, шаблону файла).

С помощью *RFM.iQ* можно выполнять определённые действия на удалённом устройстве в режиме реального времени: контроль за статусом данных, запуск программ, передача информации и др.

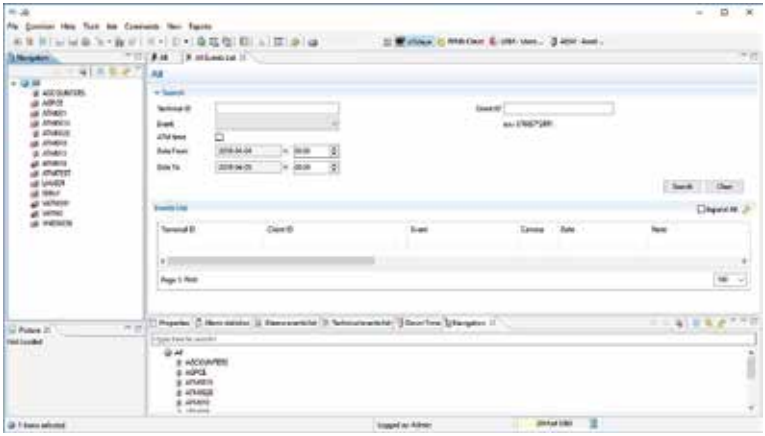
Кроме того, предусмотрена возможность передачи электронных журналов, фотографий, видеозаписей и другой информации с удалённого терминала на сервер сбора данных, а также их хранения и архивирования.

***ATMeye Module* (*Desktop*)** обеспечивает удалённое управление и мониторинг подсистемы АТМ платформы *ATMeye.iQ*. Все выполняемые с *Desktop* операции применяются непосредственно к указанной подсистеме *ATMeye.iQ*.

Чтобы открыть модуль ***ATMeye*,** следует нажать кнопку панели инструментов ***Open Module*** и выбрать пункт «***Other***»; далее выбрать пункт «***ATMeye***» из списка – и двойным кликом (или простым кликом и нажатием «***OK***») открыть модуль.



Ил. 11. Выбор перспективы в ATMeye Module (Desktop).



Ил. 12. Главный экран ATMeye Module (Desktop).

4.1.1. Основные функции *ATMeye.iQ*

Система видеомониторинга *ATMeye.iQ* является мультивендорным решением, полностью совместимым с последними версиями аппликационного программного обеспечения для устройств самообслуживания от основных производителей банкоматов вне зависимости от типа и модели устройства, надёжно защищающим оборудование и персональные данные клиентов банка.
ATMeye.iQ осуществляет дистанционный видеомониторинг в режиме реального времени и централизованное управление сетью терминалов самообслуживания.

Ил. 13. ATMeye.iQ – надёжное решение для защиты устройств самообслуживания

С её помощью возможна обработка и распознавание вредоносных действий (вандализм, мошенничество) и дальнейшее извещение оператора с предоставлением соответствующей информации.

ATMeye.iQ предоставляет такие функции, как:

- **Фото- и видеозапись событий**. При выполнении любой операции на устройстве ведутся фото- и

видеосъёмка пользователя и его действий, что помогает составить детальный отчёт о проведении каждой транзакции;

- **Фото- и видеозапись после срабатывания датчиков.** В момент срабатывания установленных на устройстве самообслуживания датчиков активируются фото- и видеозапись, что позволяет составить полный отчёт о тревожном событии.

Ил. 14. Процесс работы ATMeye.iQ во время операций на банкомате.

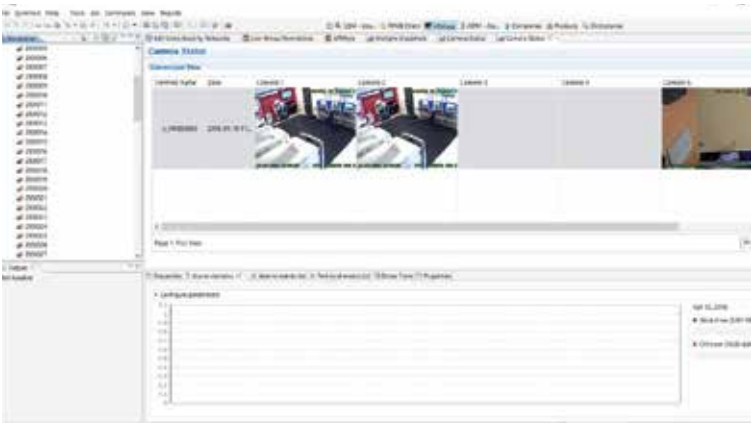
Ведение видеосъёмки до и после события. Обеспечивается возможность фото- и видеозаписи до и после конкретной транзакции или другого действия на устройстве, что помогает восстановить картину произошедшего;

Просмотр видео в режиме реального времени. Реализована возможность получить мгновенный доступ к потоковому видео и снимкам камер конкретных устройств;

Проверка рабочего состояния камер. По запросу для проверки работоспособности и корректности настроек камер можно получить тестовые снимки (*multiple snapshot*);

Поддержка различных типов камер. Система поддерживает до 4 внутренних USB или аналоговых камер, а также до 12 внешних IP-камер, что позволяет фиксировать работу считывателя карт и диспенсера, а также зону сейфа, лицо клиента и прилегающую территорию;

Настройка режимов работы камеры. Камеры могут работать в различных (дневной / ночной) режимах по установленному расписанию, позволяя получать чёткие и качественные снимки в любое время суток.



Ил. 15. Статус камер в системе ATMeye.iQ.

Камера делает от 4 до 10 снимков в секунду. То есть, можно получать точные данные с места события, причём объём передаваемых данных невелик. Благодаря этому можно с точностью до десятых долей секунды сопоставить временные данные («тэги») операций, совершаемых по определённой авторизированной банковской карте, с фотоснимками. Полученные данные о фотоснимках сохраняются в банкомате. Экспорт файлов происходит регулярно в соответствии с установками каждого банка [29].

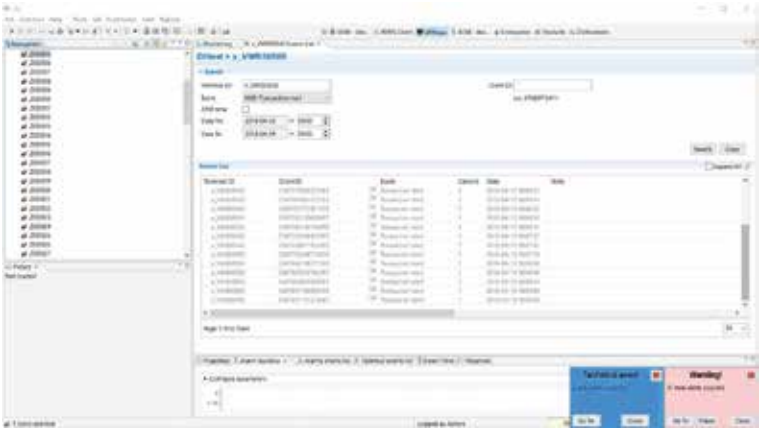
Поддерживаемое разрешение фото/видео: 320x240, 352x288, 640x480, HD

Средний размер снимка с разрешением 320x240 (в формате *JPEG*) составляет 10-20 КБ

Система располагает различными датчиками реагирования и уведомления:

Широкие возможности выявления угроз. Реализована возможность подсоединить к устройству любые типы датчиков (удара, вибрации, наклона, дыма или температуры и др.), а также специальные устройства, предотвращающие мошеннические действия;

Отслеживание тревожных событий в режиме реального времени. Уведомления о срабатывании датчиков мгновенно приходят ответственному сотруднику банка, что способствует оперативному реагированию на событие;



ИИл. 16. Уведомление о срабатывании датчиков.

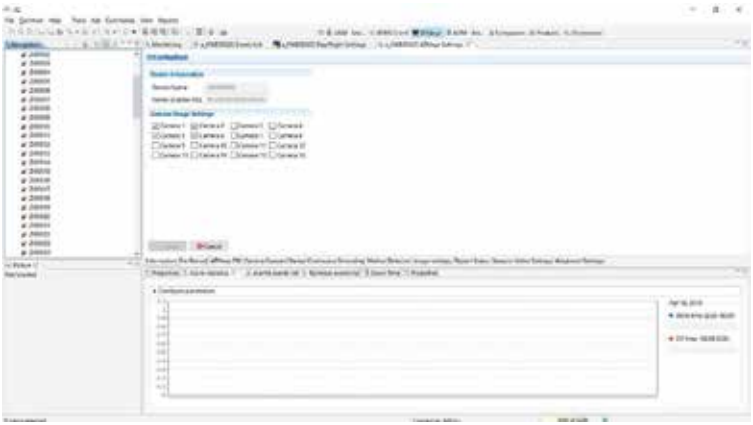
Реакция на закрытие камеры. В случае закрытия или отключения камеры ответственным сотрудникам банка приходят автоматические сообщения о тревожном событии, что даёт возможность предотвратить более серьёзные последствия;

Мобильные уведомления. Экстренные сообщения о любых нештатных ситуациях могут быть отправлены в режиме реального времени на мобильные устройства через приложение *Mobile ATMeye.iQ*.

Ил. 17. Датчики реагирования и уведомления системы видеомониторинга ATMeye.iQ.

Кроме того, система обеспечивает дополнительные функции:

Дистанционная настройка камер. Реализована возможность удалённой настройки камер без выезда сотрудников сервисной службы к устройству. Это позволяет выбрать оптимальный режим съёмки (дневной или ночной), а также установить яркость, чёткость и другие параметры.



Ил. 18. Интерфейс дистанционной настройки камер.

Шифрование и защита передаваемых данных. Обмен данными в системе ведётся в зашифрованном виде по защищённому каналу связи.

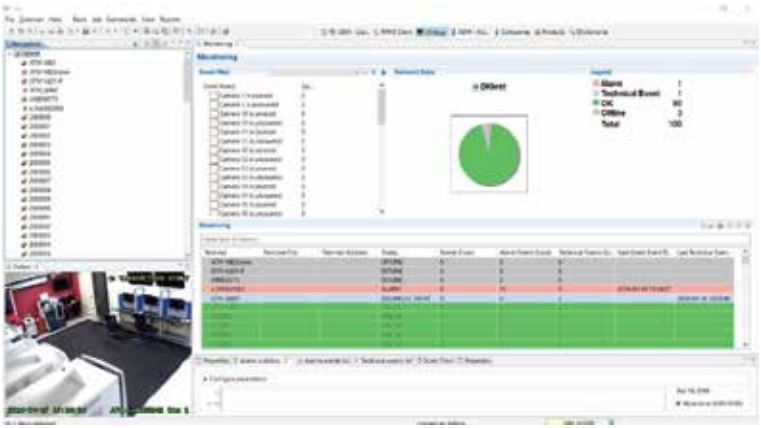
Централизованное управление файлами. Интеграция с решением *RFM.iQ* позволяет передавать файлы (фотографии, видеозаписи, электронные журналы, обновления ПО) между удалёнными устройствами самообслуживания, рабочим местом администратора и сервером сбора данных.

Удалённое обновление программного обеспечения. Обновление ПО по сети происходит централизованно без выезда сотрудников сервисной службы.

Планирование заданий. Обеспечение функций обмена данными и архивирования фотографий, видеозаписей и электронных журналов по расписанию или заданному алгоритму.

Для мониторинга реализованы следующие функции:

Единый интерфейс для всех событий системы. События со всех устройств выводятся на один экран в понятном виде, позволяя получить полную картину работы всей системы.



Ил. 19. Общий мониторинг в системе ATMeye.iQ

Проактивная система уведомлений. Сообщение о событиях приходят всем ответственным сотрудникам по нескольким доступным каналам оповещения, что делает работу персонала более оперативной.

Удобный поиск устройства самообслуживания. Для оптимизации работы оператора реализована функция сортировки и поиска конкретного устройства по филиалу, городу, региону или другим параметрам.

Удобный поиск транзакции. Система позволяет найти интересующую транзакцию по номеру карты, событию, дате и другим параметрам, заметно облегчая работу службы поддержки банка.

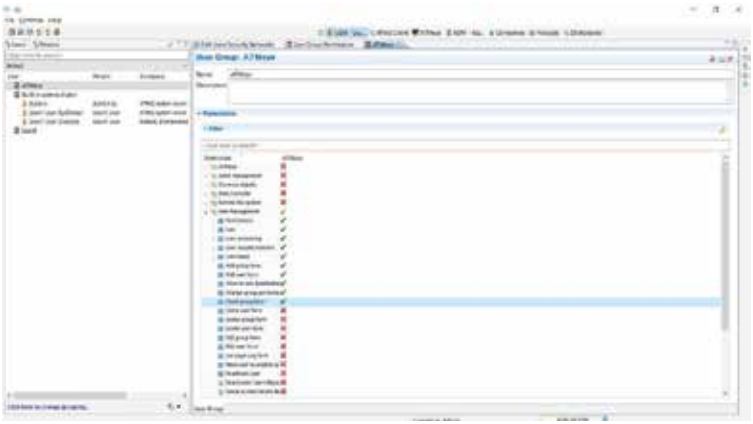
Проверка сетевого подключения устройства. Оператор в режиме реального времени получает информацию о текущем рабочем статусе устройства самообслуживания. Это позволяет оперативно реагировать в случае возникновения технических проблем.

Принудительный захват или отказ в обслуживании карты. Банковская карта, внесенная в «чёрный список» (*black list*) банка, может быть удержана устройством самообслуживания в случае необходимости. Оператор системы будет уведомлён о таком событии мгновенным сообщением.

Маскировка номера карты. Номер банковской карты маскируется в системе, обеспечивая полную конфиденциальность персональных данных клиента.

Автоматизированные рабочие места. В системе *ATMeye.iQ* создано несколько рабочих мест с набором уникальных функций для более эффективного выполнения задач и поддержания необходимого уровня безопасности.

Администратор системы имеет возможность управлять правами пользователей, администрировать лицензии, импортировать данные из других систем, проводить резервное копирование и восстановление информации, наблюдать за состоянием сети, планировать и проводить работы, а также получать разнообразную статистику.



Ил. 20. Интерфейс, где устанавливаются права и роли в системе ATMeye.iQ.

Оператор системы обладает всем необходимым функционалом для получения информации о работе устройств самообслуживания, действиях пользователей, не забранных картах или наличных средствах, а также обо всех транзакциях на каждом устройстве самообслуживания.

Оператор имеет возможность в любой момент подключиться к устройствам наблюдения и вести мониторинг помещения или зоны вокруг определённого банкомата. Благодаря технологии распознавания лиц система способна сопоставить лица, попадающие в поле съёмки, с базой имеющихся данных – и при совпадении уведомить оператора об обнаружении персон из «чёрного списка» банка или разыскиваемых лиц (например, при интеграции с базой данных полиции). Таким образом, эффективность работы службы безопасности многократно повышается [29].

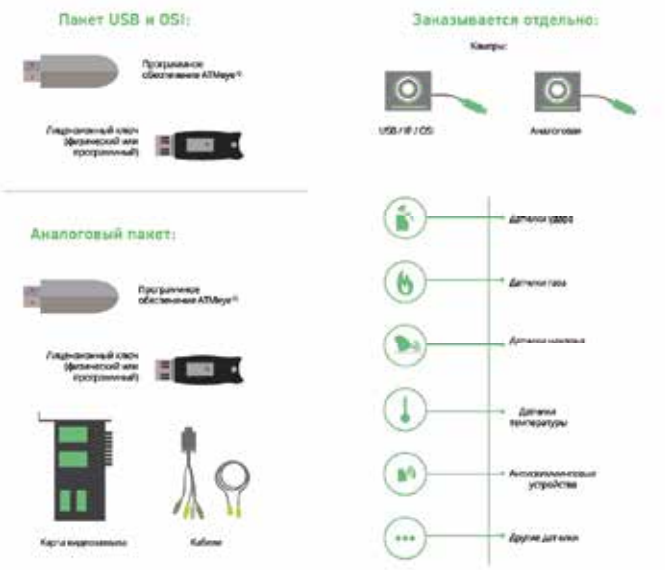
Сотрудник службы безопасности может получать мгновенные уведомления обо всех тревожных событиях (попытках взлома, порче устройств самообслуживания и многих других). При этом реализована возможность формировать отчёты со статистикой таких событий для анализа и дальнейшего принятия решений.

ASM.ATMeye.iQ. Результатом интеграции устройства антискимминга с *ATMeye.iQ* является современное решение *ASM.ATMeye.iQ* для борьбы с самыми изощренными случаями мошенничества. *ATMeye.iQ* работает с любым типом антискимминговых устройств, а также с решениями логической безопасности (системами *фрод-мониторинга*).

ASM.ATMeye.iQ предоставляет следующие функции:

Мгновенное оповещение сотрудников. При обнаружении установки набора скимминговых инструментов система *ATMeye.iQ* в режиме реального времени рассылает уведомления об этом событии на рабочие компьютеры или на мобильные устройства сотрудников банка. При этом преступные действия фиксируются камерами, а фотографии и видеозаписи передаются сотрудникам службы безопасности.

Предоставление подробных отчётов. По запросу или заранее заданному расписанию предоставляются сгенерированные отчёты со статистикой попыток установки скиммеров на устройствах самообслуживания, что позволяет проанализировать общую картину безопасности сети.



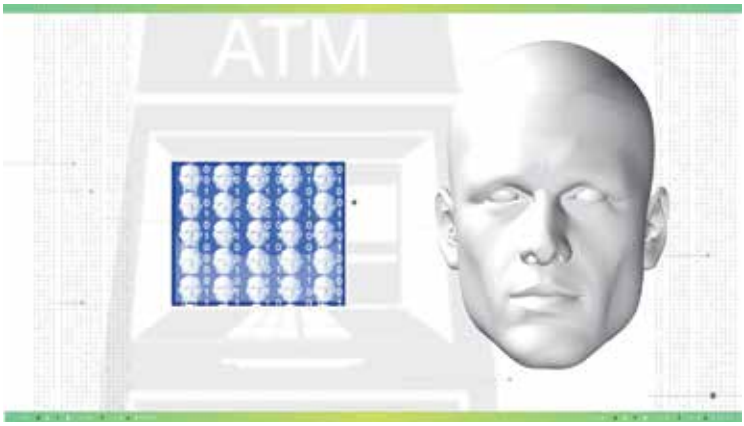
Ил. 21. Комплект поставки системы ATMeye.iQ.

Компания *BS/2* предоставляет своим клиентам:

- Продажу или аренду необходимого набора устройств, в который входят карты видеозахвата, различные датчики и другие компоненты по запросу.
- Внедрение, поддержку и обновления серверного и терминального АПК системы *ATMeye.iQ* и приложения *Mobile ATMeye.iQ*.

В разделе 2.5.8 уже отмечалась значимость биометрических методов идентификации для самообслуживания клиентов как одного из главных трендов в развитии современных банковских технологий. При этом решения по распознаванию образов органично сочетаются с задачами видеобезопасности, т.к., многие устройства самообслуживания уже оснащены видеокамерами. В этом плане примечательно решение о стратегическом партнёрстве между *BS/2* и *VisionLabs*, одним из лидеров рынка по внедрению технологии распознавания

образов в мире, и создании линейки межбанковских сервисов идентификации на базе системы *ATMeye.iQ* и платформы *LUNA*.



Ил. 22. Применение технологии распознавания лиц в ATMeye.iQ для защиты банкоматов.

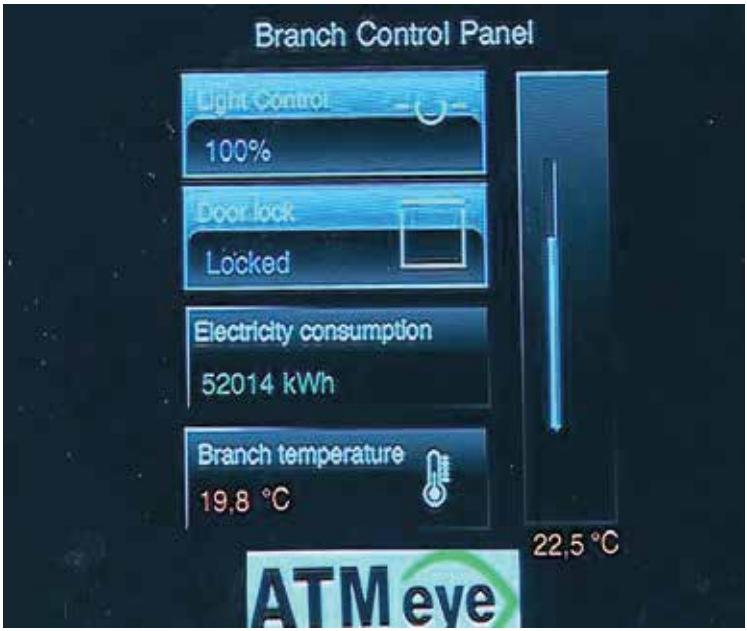
Финансовые учреждения стремятся, с одной стороны, дать клиенту как можно больше целевой рекламы во время выполнения им стандартных действий на банкомате, а с другой, обеспечить его дополнительными сервисами (возможностью оплачивать различные услуги, совершать обмен валюты и др.). Для этих целей в 2017 году система *ATMeye.iQ* была интегрирована с текущей версией *ProFlex 4.0* от компании *Diebold Nixdorf*.

4.2. *Brancheye.iQ* – безопасность и видеомониторинг отделения банка

С помощью *ATMeye.iQ* можно объединить дистанционное управление различными каналами финансовых услуг и безопасностью в филиалах банка и контроля всех процессов,

связанных с обеспечением жизнедеятельности (системы отопления и кондиционирования, электрические сети и т.д.) в режиме реального времени.

Именно с этой целью разработано решение *Brancheye.iQ*, призванное осуществлять видеонаблюдение за отделениями банка и надёжную организацию безопасной работы банковских и других офисов.



Ил. 23. Главный вход в приложение Brancheye.iQ

Brancheye.iQ способствует повышению уровня безопасности банковского отделения (предупреждение краж, вандализма, системных ошибок, др.), также оказывается полезным при управлении претензионной работой с клиентами. Оно может быть интегрировано с другими системами контроля управления здания. Его внедрение даст снижение операционных и эксплуатационных затрат.

Перечислим основные функции *Brancheye.iQ*:

- гибкая система поиска видеосюжетов / снимков и администрирование архива;
- мгновенная реакция на сообщения сенсоров, фиксирующих необычные события; анализ снимков и потокового видео;
- автоматические сигналы тревоги на подозрительные события;
- генерирование отчётов и аналитических данных;
- управление правами пользователей и доступа;
- простая интеграция с другими ИТ-системами;
- интеграция с банкоматами и платформами различных производителей (*multivendor*);
- возможность управления посредством любых мобильных устройств – смартфонов, планшетных компьютеров, через Интернет;
- дистанционный мониторинг;
- устранение ошибок в системе коммуникации;
- управление системой согласно расписанию;
- поддержка до 16 различных источников видеоинформации;
- контроль системы управления зданием;
- интеллектуальное измерение: мониторинг использования электричества, газа, воды, систем отопления и охлаждения;
- распознавание лиц.

Cash Management.iQ

Автоматизация, оптимизация, управление и контроль за оборотом наличности

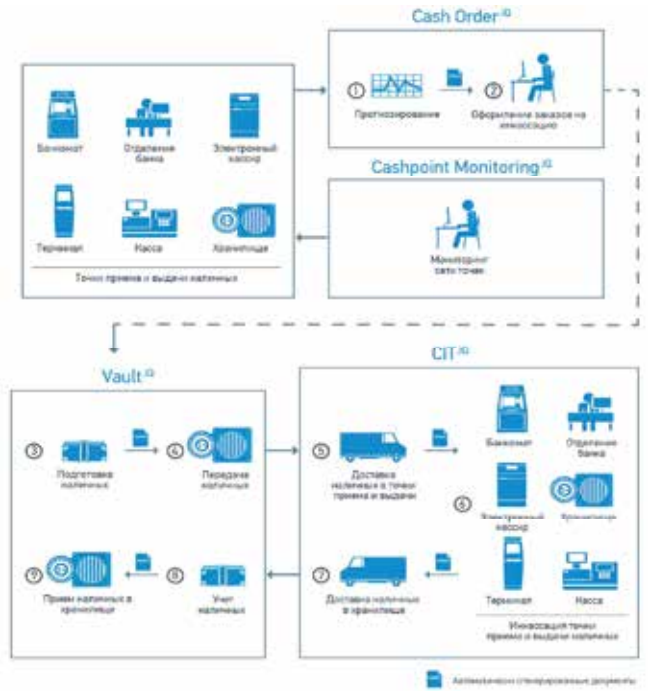
Cash Management .iQ
.iQ Family Product

Cash Management.iQ – программный продукт, предназначенный для решения задачи эффективного распределения денежных средств в точках приема и выдачи наличности: банкоматах и других устройствах самообслуживания, а также в банковских хранилищах, отделениях банков, почты и розничных сетях.

4.3. *Cash Management.iQ* – оптимизация денежных потоков, управление и контроль

Cash Management.iQ – продукт семейства «*.iQ*» для автоматизации процессов, связанных с распределением наличных денег во всех точках их приема и выдачи (банкоматы, электронные кассиры, хранилища, расчётно-кассовые отделения, платёжные терминалы, инфокиоски и др.).

Это состоящее из четырёх дополняющих друг друга модулей мультивендорное решение позволяет поддерживать оптимальное количество денежных средств во всей сети и оптимизировать процессы, связанные с движением наличности.



Ил. 24. Рабочий процесс Cash Management.iQ

С помощью модуля *Cash Order.iQ* можно дать прогнозы потоков наличности – т.е., прогнозировать потребности в наличности, планировать и оформлять заказы на инкассацию для устройств самообслуживания и банковских отделений, а также устанавливать лимиты на загружаемые суммы и остатки наличности в точках: с этой целью используется механизм прогнозирования, построенный на основе нейронных сетей.

Тем самым можно определить срок проведения инкассации для каждой отдельно взятой точки приёма / выдачи на основе статистических данных движения наличности.

Модуль *Cashpoint Monitoring.iQ* предназначен для мониторинга баланса наличности в реальном времени в точках приема/выдачи с детализацией по валютам и номиналам. При этом возможен мониторинг состояния всей сети точек и отдельно выбранных объектов.

Модуль *Vault.iQ* служит для мониторинга баланса наличности в хранилищах с детализацией по валютам и номиналам. Также можно осуществить планирование и оформление заказов на пополнение и вывоз наличности. Модуль обеспечивает контроль состояния наличности в хранилищах на начало и конец операционного дня.

С помощью модуля *CIT.iQ* осуществляются формирование бригад инкассаторов, контроль за их работой, формирование и оптимизация маршрутных листов, контроль за доставкой наличности до объектов назначения (хранилищ и филиалов банков, устройств самообслуживания, частных лиц), а также контроль за проведением инкассаций.

С помощью дополнительного модуля бизнес-аналитики *Dashboard.iQ* имеется также возможность генерирования отчётности на каждой стадии процесса. В зависимости от бизнес-процесса и потребностей организации возможно

использование, внедрение и интеграцию как полного пакета *Cash Management.iQ*, так и отдельных модулей или их комбинаций.

Таким образом, решение *Cash Management.iQ* способствует снижению затрат на поддержку процесса распределения наличных денежных средств, временных затрат на планирование и генерацию заказов на инкассации; контролирует состояние сети точек обслуживания в режиме реального времени с настраиваемым механизмом оповещений; упрощает организацию процессов распределения наличных, а также своевременно реагирует на изменения требований рынка банковских услуг в части операций с наличными.

Кроме того, обеспечиваются контроль за качеством выполнения требований инструкций, оптимизация инкассаций по критерию стоимости, автоматизация и документооборот по работе с наличными, управление рисками (нахождение компромисса между безопасностью и операционной деятельностью), аналитика бизнес-процессов, выявление трендов показателей качества.

Использование перечисленных выше инструментов способствует доступности точек приёма / выдачи наличных и существенному уменьшению числа нарушений.

Для каждого отдельного внедрения расчёт возврата инвестиций (*return on investment; ROI*) осуществляется с учётом влияющих факторов – таких, как стоимость инкассации, замороженных денежных средств, их страхования и др.

SmartSafe.iQ

Система управления электронными кассирами

SmartSafe.iQ

.iQ Family Product

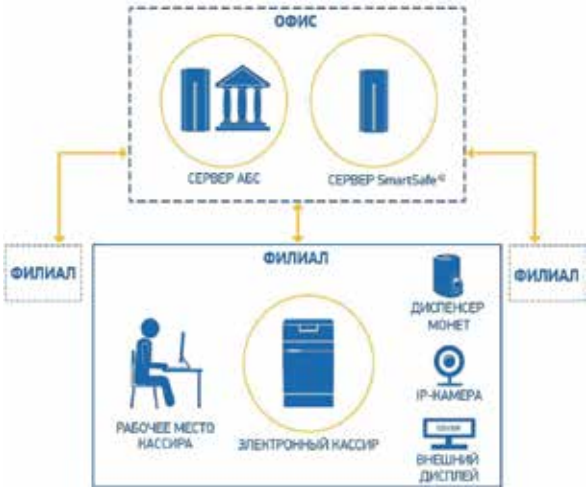
Система **SmartSafe.iQ** предназначена для управления электронными кассирами и дополнительным периферийным оборудованием, а также автоматизации операций, связанных с приемом и выдачей наличных средств в отделениях банков, почты и в других организациях.

4.4. *SmartSafe.iQ* – автоматизация и администрирование рабочих мест кассиров

Интегрированная в автоматизированную банковскую систему (АБС) банка система *SmartSafe.iQ* предназначена для управления электронными кассирами различных производителей, а также для администрирования рабочих мест приёма и выдачи наличных.

Централизованное управление *SmartSafe.iQ* позволяет осуществлять централизованный контроль за всеми операциями с наличностью.

В целях повышения безопасности и для осуществления функции видеонаблюдения система интегрирована с *ATMeye.iQ*, которая по различным событиям (операциям с наличными) позволяет проводить фоторегистрацию зоны рабочих мест кассиров (сейфа).



Ил. 25. Схема решения SmartSafe.iQ

Мультивендорное решение *SmartSafe.iQ* совместимо с моделями от основных мировых производителей *Wincor Nixdorf, CTS,*

DoCash, Glory, De La Rue, Talaris, Vertera – причём их перечень постоянно расширяется. Интеграция с любым новым типом оборудования занимает в среднем 2-3 месяца.

SmartSafe.iQ поддерживает одновременную работу с несколькими валютами различных стран мира, включая работу электронных кассиров с банкнотами 128 различных номиналов. Во время работы гарантируется безопасность данных, благодаря их передаче с применением протокола *SSL*. Поддерживается генерирование сертификатов безопасности в системе, а также загрузка из внешних систем.

Для банков, стремящихся к полной автоматизации рабочих мест кассиров, в *SmartSafe.iQ* предусмотрена поддержка монетного диспенсера, что позволяет выдавать всю необходимую сумму купюрами и монетами.

Возможность объединять рабочие места кассиров в общую компьютерную сеть позволяет персоналу быстро переключаться между сейфами и объединять их с другими периферийными устройствами (диспенсер монет, внешний дисплей, камера, считыватель карт и др.) с применением протокола *SSL*, формируя необходимую гибкую конфигурацию.

Благодаря дополнительному модулю бизнес-аналитики система *Dashboard.iQ* позволяет создавать все необходимые отчёты в удобной форме.

Ил. 26. Электронные кассиры Diebold Nixdorf

Решение *SmartSafe.iQ* предназначено для выполнения следующих основных задач:

- автоматизированные приём и выдача наличных клиентам;
- автоматизированные загрузка и выгрузка наличных (инкассации);
- контроль и мониторинг процедур в течение рабочего дня;
- мониторинг денежной наличности в режиме реального времени;
- оперативный доступ к различным отчётам;
- администрирование программного и аппаратного обеспечения.

Применительно к услугам банка для своих клиентов система обеспечивает:

- выдачу и приём наличных; оплату товаров и услуг;
- обмен валюты с зачислением остатка на банковский счет;
- получение наличных снятием с любого (внебанковского) счета;
- предоставление информации из внешних информационных и биллинговых систем;
- пересчёт пачки наличных; размен наличных на более крупные / мелкие купюры.

Также можно получить полную отчётность, включающую кассовый отчёт по электронному кассиру, по инкассациям электронного кассира, по операциям за выбранный период, по обороту электронных кассиров за данный период, по остатку денежных средств, техническому состоянию оборудования с точностью до узла и т.д.

Система поддерживает мониторинг текущего баланса сети электронных кассиров – а, благодаря механизму мультиязычности, есть возможность создавать пользовательский интерфейс и отчётность на выбранном языке.

4.4.1. *Mobile SmartSafe.iQ* – мобильное приложение для проведения операций с наличными

Mobile SmartSafe.iQ – новая платёжная инфраструктура самообслуживания на базе электронных кассиров (*automated teller safe; ATS*) и смартфона. Главными особенностями *Mobile SmartSafe.iQ* являются: удобство использования, расширенный функционал, высокий уровень безопасности, снижение стоимости точки обслуживания и нагрузки персонала

операционного зала банковского отделения. Конечным пользователям *Mobile SmartSafe.iQ* предоставляет широкий спектр банковских услуг по проведению операций с наличными (приём и выдача наличных, в том числе, с зачислением на банковский счет, оплата услуг, обмен валют и т.д.).

Система позволяет объединить функции рециркуляционного банкомата, платёжного киоска самообслуживания, автомата по обмену валют и предоставляет все эти услуги в удобном интерфейсе личного смартфона.

Mobile SmartSafe.iQ позволяет:

- обеспечить клиентам комфортную среду для выполнения операций с наличными на базе смартфона;
- дополнить решения самыми инновационными функциями (инструкции пользования на базе дополненной реальности (*augmented reality*), выдача наличных под обязательства мобильного оператора и т.п.);
- снизить стоимость оборудования точки самообслуживания;
- уменьшить рабочую нагрузку банковских кассиров банка за счёт направления части клиентов на устройства самообслуживания;
- снизить цены на электронные кассиры за счёт более массового производства;
- осуществить перевод электронных кассиров в разряд устройств массового обслуживания;

Ил. 27. Примеры пользовательского интерфейса приложения Mobile SmartSafe.iQ.

Перечислим основные функции и преимущества приложения *Mobile SmartSafe.iQ*.

Предоставление клиентам банка следующих услуг:

- выдача и приём наличных;
- оплата товаров и услуг методом приёма наличных;
- обмен валюты с зачислением остатка на банковский счёт;
- получение наличных снятием с любого (внебанковского) счёта (*Cash Anywhere*);
- предоставление информации из внешних информационных и биллинговых систем;
- пересчёт пачки наличных;
- размен наличных купюрами больших или меньших номиналов (*change*).

С другой стороны, приложение предполагает получение персоналом полной отчётности (базовый перечень отчётов дополняется в соответствии с необходимыми формами),

в т. ч., кассовый отчёт по сейфу, отчёт по инкассациям сейфа, отчёт по операциям за выбранный период и т.п.

Приложение имеет следующие функции по мониторингу:

- мониторинг сети сейфов;
- доступность сейфов и серверов по сети передачи сообщений;
- текущий баланс сейфов;
- техническое состояние оборудования с точностью до узла.

Cash-in Box.iQ

Решение для депозита наличности

Cash-In Box .iQ

.iQ Family Product

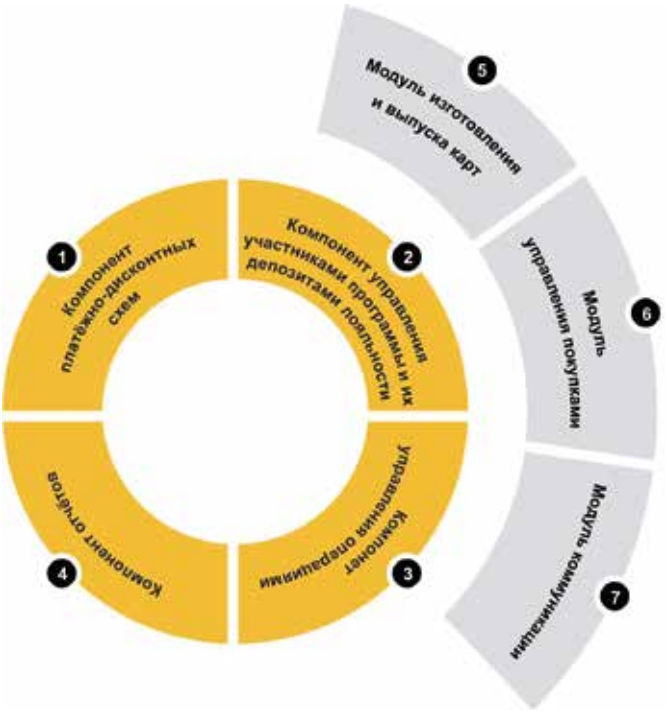
Решение **Cash-In Box**.iQ представляет собой надежную депозитную машину, интегрированную с ИТ-системой банка, обслуживающего торговую точку, а также эффективные и удобные инструменты для мониторинга и контроля работы всех подключенных устройств самообслуживания.

4.5. *PayLo* – решение для управления программами платежей и лояльности

Разработанная и поддерживаемая компанией *ASHBURN International* (группа *Penki Kontinentai*) модульная система по управлению сценариями платежей и лояльности *PayLo* является универсальным инструментом управления платежами и схемами лояльности, который может быть интегрирован в кассы, либо реализован на отдельных платёжных терминалах [28].

Ил. 28. Логическая схема программы кросс-лояльности.

Система *PayLo* ориентирована на потребности различных продавцов в сфере создания программ и схем лояльности. Система включает все этапы обслуживания программ лояльности, начиная с фазы первичной идентификации клиента до создания схем лояльности, обработки операций лояльности и анализа накопленных программой данных.



Ил. 29. Компоненты и модули решения PayLo.

Участники программы лояльности могут управлять схемами лояльности посредством пользовательского интерфейса в сети Интернет.

В числе основных возможностей пользовательского интерфейса *PayLo* можно выделить:

- ввод в систему и редактирование данных об участниках программы лояльности;
- установка и изменение параметров схем лояльности;
- доступ к информации о составляющих схем лояльности;
- мониторинг операций лояльности в режиме реального времени.

Система *PayLo* состоит из целевых компонент и модулей, включая все этапы внедрения и обслуживания программы лояльности (ил. 29).

Компонент управления схемами платежей и лояльности предназначен для создания и управления сценариями лояльности, осуществления логики лояльности.

Компонент управления участниками программы и их счетами лояльности отвечает за ведение базы данных участников программы (физических / юридических лиц), создание новых платёжных счетов и счетов лояльности, блокировку карт, предоставление кредитных лимитов, назначение схем лояльности и т.д.

Компонент управления операциями обеспечивает авторизацию и коррекцию платежных операций и операций лояльности, накопление истории.

Компонент отчетов предназначен для генерирования периодических и специальных отчётов в различных разрезах с использованием накапливаемых системой данных, определяющих демографию, активность, поведение и т. д. клиентов (участников программы лояльности).

Модуль изготовления и выпуска карт отвечает за изготовление и выпуск карт (от сканирования анкет до выдачи карты).

Модуль управления покупками поддерживает управление сложными сценариями программ платежей и лояльности, в которых используется ассортимент товаров / услуг заказчика.

Модуль коммуникации является маркетинговым инструментом для поддержки прямой связи с участниками программы лояльности посредством *SMS*-сообщений и электронной почты.

Как известно, для идентификации клиентов в торговых точках используются различные устройства:

- *POS-терминалы*;
- *NFC-сканеры* (интегрированные в / подключенные к POS-терминалам);
- кассы со встроенными считывателями магнитной полосы карты;
- считыватели карт, работающие в сочетании с мобильным устройством (смартфоном или планшетным компьютером);
- идентификация «виртуальных карт» посредством мобильного устройства (смартфона или планшетного компьютера).

При внедрении программ лояльности с помощью *PayLo* могут использоваться различные средства и устройства идентификации клиента. Среди них следует отметить платёжные карты и карты лояльности (считывание магнитной полосы, штрих-кода, *QR*-кода или *NFC*).

Идентификация клиентов также может быть проведена по «виртуальной карте» в смартфоне или планшетном компьютере. Кроме того, *PayLo* даёт возможность привязки распознавания образа клиента к определённым программам лояльности.

ASHBURN International работает в соответствии с гарантирующим физическую и виртуальную безопасность данных стандартом высочайшего уровня *PCI DSS Level 1*, обеспечивающим безопасность данных международных платежных карт. Данный стандарт включает жесткие требования к техническому оборудованию и программному обеспечению, внутренним процессам компании, ИТ-архитектуре, процессу разработки программного обеспечения, документации.

4.6. *Mobile ATMeye .iQ* – платформа для мобильных решений

Mobile ATMeye iQ — приложение для смартфона или планшета, позволяющее мгновенно получать уведомления о любых подозрительных действиях на устройствах самообслуживания или в непосредственной близости от них.

Ил. 30. Приложение Mobile ATMeye iQ: уведомления о прикрытии камеры конкретного терминала.

Приложение *Mobile ATMeye iQ* предлагает надёжные инструменты для действий в нештатной ситуации:

- запрос по текущему статусу устройства самообслуживания и его компонентов;
- просмотр фотографий и видеозаписей в режиме реального времени, а также материалов, зафиксированных до и после события.

Mobile ATMeye iQ обеспечивает следующие функции:

- оповещение сотрудников банка по SMS, электронной почте или иными способами;
- вызов работников службы безопасности;

- запуск любого запрограммированного процесса на устройстве самообслуживания;
- включение сигнализации;
- остановка и запуск приложения устройства самообслуживания;
- перезагрузка устройства самообслуживания.

VTM.iQ

Решение для видеобанкинга

VTM.iQ Family Product

VTM.iQ – решение для дистанционного банковского обслуживания, позволяющее снизить расходы на предоставление различных банковских услуг, повысить их качество и укрепить лояльность клиентов.

4.7. *VTM.iQ* – решение для удалённого получения банковских услуг

VTM.iQ представляет собой совершенно новый технологический подход к оказанию финансовых услуг, позволяющий кардинально преобразовать работу с клиентами.

VTM.iQ предназначен для проведения банковских и платёжных операций и включает в себя уникальную технологическую концепцию терминала *CuRiE* (*Customer Rich Experience*), электронный кассир с функцией рециркуляции наличности *CS 6060* от компании *Diebold Nixdorf*, а также программные решения и системную интеграцию от компании *BS/2*.

VTM.iQ легко интегрируется с основными банковскими системами (*АБС, ЦДО, «Процессинг»*) и предоставляет дополнительный канал обслуживания клиентов, ориентированный на т.н. «продвинутых» компьютерных пользователей, позволяющий им экономить своё время – и самостоятельно (или при содействии оператора центра дистанционного обслуживания) выполнять практически любые банковские операции, вести онлайн-видеоконсультации по работе с *VTM.iQ* и предлагаемым банком услугам, получать персонализированную информацию по услугам банка, заказать и тут же получить банковскую карту, осуществлять выплаты по кредиту.

Решение позволяет пользоваться различными механизмами идентификации личности (при помощи банковской карты, скана удостоверения личности, отпечатка пальца), заключать договор на банковское обслуживание, открыть счёт, оформить и подписать кредитный договор и получить деньги на расчётный счёт / кредитную карту / наличными, проверить баланс счёта и получить выписку по обороту за выбранный период времени, внести наличные средства, пополнить расчётный или карточный

счёт, получить наличные с расчётного или карточного счёта, выполнять платёжные операции наличными, с платёжной карты переводом средств со счёта, оплатить счета за коммунальные услуги, связь, транспорт, купить билеты, ваучеры и т. д., заблокировать карту в случае утери или кражи, изменить PIN-код карты.

VTM.iQ представляет собой симбиоз нескольких функциональных систем и предлагает интерактивный подход к работе с клиентами.

Использование видеосвязи высокой чёткости (*HD*) для общения со специалистами центра дистанционного обслуживания (ЦДО), внедрение таких технологий, как сканирование отпечатков пальцев, кодирование собственноручной подписи, контактная и бесконтактная идентификация банковской карты, финансовое самообслуживание (аналогичное с работой банкоматов), интегрированная система видеонаблюдения позволяют не только повысить безопасность проводимых операций, но также оптимизировать процессы работы с наличными.

Наряду с традиционными банковскими функциями комплексное решение *VTM.iQ* предоставляет клиентам услуги удалённого виртуального сотрудника (оператора ЦДО), консультирующего клиентов, помогающего им взаимодействовать с оборудованием. Совместная работа оператора и клиента позволяет банку предлагать более безопасные, удобные и профессиональные финансовые, страховые и административные услуги, повышая этим уровень удовлетворенности клиентов.

Оптимизация работы персонала банка путём организации «Центра компетенции» и использование *VTM.iQ* позволяет банкам предоставлять клиентам высококачественные услуги вне зависимости от расположения филиалов и наличия в них квалифицированного персонала, оптимизировать и минимизировать количество, а также размеры банковских

отделений и (соответственно) значительно сократить затраты на обслуживание клиентов без ущерба его качеству.

Ил. 31. Основные компоненты АПК VTM.iQ

VTM.iQ является идеальным решением как для современного поколения, предлагающее простое и быстрое обслуживание, так и для людей с ограниченными возможностями у которых появляется возможность совершать финансовые операции при помощи сотрудника ЦДО.

Аппаратно-программный комплекс *VTM.iQ* предлагает новые впечатляющие меры безопасности: видеокамеры высокого разрешения, защитные программные решения (*Anti-Skimming, Encrypted PIN-pad*), которые закрывают потенциальные бреши в системе безопасности, улучшают доступность системы и помогают завоевать доверие клиентов.

Ил. 32. Многофункциональные терминалы VTM.iQ.

Устанавливая *VTM.iQ* в отделениях банков, круглосуточных пунктах самообслуживания, жилых и коммерческих помещениях, залах ожидания аэропортов и вокзалов, гостиницах и труднодоступных отдалённых сельских районах и поселках, появляется возможность значительно расширить зоны обслуживания и стать ближе к клиентам.

4.8. Перспективы применения видеоаналитики на платформе *ATMeye.iQ* в «умных домах» и «умных городах»

В ряде мегаполисов мира уже развёртываются проекты «умного города» (*smart city*), что предусматривает создание гибридной автоматизированной системы для решения всех технических задач городского хозяйства. Эта система должна включать комплекс программно-аппаратных средств (видеокамеры, приборы учёта расхода ресурсов, экстренная голосовая связь и т.д.) и организационных мер по защите видео- и технической безопасности, а также для управления объектами городского хозяйства.

«Умная» эффективность в современном городе требует среды, способной смягчать, контролировать и реагировать на угрозы безопасности. Поскольку уровень городского риска увеличился за счёт глобальных неустойчивостей, применение технологий для защиты городских центров расширилось до использования множества различных датчиков, подключённых через «*Интернет вещей*».

Современный город представляет собой сложную многоуровневую структуру, состоящую из разных подсистем – транспортной, телекоммуникационной, электро- и водоснабжения, а также многих других, которые функционируют и взаимодействуют между собой. Поэтому для контроля работы всех городских систем, обеспечения безопасности городской инфраструктуры, получения и архивирования информации обо всех важных событиях и оперативного предоставления этой информации всем заинтересованным службам, необходима комплексная информационная система с развитыми функциями. В их числе – функции сбора и накопления, интеграции, видеоаналитики, группировки разнородных данных от множества источников.

В настоящее время на рынке средств домашней безопасности работает множество крупных компаний – таких, как *Comcast, Time Warner Cable* и *AT&T*. По мнению ведущих экспертов, это обусловлено тем, что безопасность остаётся ведущим направлением в сфере «умного дома».

Согласно данным исследовательской компании *Parks Associates* о состоянии конкурентной среды в сфере безопасности в жилом секторе США, приборы для «умного дома» входят в состав 42% новых проектов по установке систем безопасности в жилых домах.

При этом интерактивные сервисы или средства удалённого контроля присутствуют в 70% инсталлируемых ныне систем безопасности для дома. В целом, такие сервисы используют более 60% американских семей, имеющих широкополосное подключение к Интернету – и получающих услуги профессионального мониторинга. Среди домашних пользователей широкополосных сетей США 23-25% имеют работающую систему безопасности и 21-23% получают услугу профессионального мониторинга. Примерно 50-60% устройств «умного дома», связанных с безопасностью, приобретаются как часть общей домашней системы.

В Европе эта среда отличается наличием большой доли устаревшего оборудования для обеспечения безопасности, и информационно-коммуникационные проекты в этом регионе, как правило, ориентированы на максимальные возможности существующих технологий при одновременной модернизации и увязывании имеющихся разрозненных систем.

Ввиду заинтересованности правительств развитых стран в использовании новейших технологий защиты безопасности, глобальный рынок безопасных городских решений должен составить к 2021 году более $20 млрд.

Рассмотренные в этой книге возможности широкие платформы *ATMeye.iQ* в плане видеоаналитики и видеобезопасности предлагают новые пути для государственных ведомств и городских служб для обнаружения угроз, смягчения их последствий и оказания им чрезвычайной помощи.

4.9. Инновационные разработки компании *BS/2* – залог её успеха на мировом рынке

Важно отметить, что комплекс *ATMeye.iQ* впервые получил награду международной промышленной ассоциации *ATMIA* (*ATM Industry Association*) *Best ATM Security Technology 2002*.

В 2017 году комплексное решение *ATMeye.iQ* удостоилось золотой медали традиционного конкурса «Продукт года», организуемого Конфедерацией промышленников Литвы. Этот приз стал уже второй наградой, полученной *BS/2* за *ATMeye.iQ* – оно уже удостаивалось золотой медали «Продукт года» в 2008 году.

В ходе ежегодного съезда партнеров крупнейшего в мире производителя банковского оборудования *Diebold Nixdorf* компания *BS/2* была удостоена престижной международной награды *Special Achievement Banking 2017* за реализованное в Азербайджане инновационное технологическое решение – тогда *BS/2* поставила одному из банков республики полностью автоматизированное банковское отделение по предоставлению финансовых услуг в режиме самообслуживания, в котором установлен аппаратно-программный комплекс *VTM.iQ*. Он включает в себя электронный кассир *CS 6060* от *Diebold Nixdorf*, многофункциональный терминал, а также специализированные программные решения от *BS/2*. Этот не имеющий аналогов аппаратно-программный комплекс подобного типа – первый не только в Азербайджане, но и других странах СНГ (в настоящее

время подобная технология от *BS/2* действует также в Казахстане).

В начале 2011 года компания *BS/2* внедрила признанные во всем мире практики по управлению ИТ-процессами *ITIL V3 (Information Technology Infrastructure Library)* и успешно прошла сертификационный аудит на соответствие стандарту *ISO 20000*.

В 2012 году компания прошла аудит и получила сертификат соответствия стандарту *ISO 27001*, что подтверждает высокое качество услуг, предоставляемых компанией *BS/2*.

На состоявшемся в 2014 году съезде партнеров компании *Diebold Nixdorf* за успешные деятельности в Грузии компания *BS/2* была удостоена приза *Best Service Banking 2013/2014*, а в категории *Special Achievement Banking 2013/2014* компания была отмечена за весьма успешные результаты продаж в Молдове. Ещё один приз – *Special Achievement Banking 2013/2014* – компания *BS/2* разделила с работающей в Азербайджане компанией *Komtec* за успешную деятельность в банковском секторе Азербайджана.

В 2016 году *Diebold Nixdorf* наградил компанию призом *Best Banking Solution 2016* за успешную реализацию проекта по модернизации и оптимизации парка банкоматов одного из крупнейших банков в Балтийских странах.

Ранее компания *BS/2* также удостаивалась таких наград от *Diebold Nixdorf* / *Wincor Nixdorf,* как *Best Banking Solution 2016, Special Achievement Banking 2013/2014, Best Banking Service 2013/2014, Best Banking Service 2012/2013* и ряд других престижных премий.

Компания *BS/2* является членом международной ассоциации *ATMIA*, представляющей мировую индустрию банковского оборудования.

Компания имеет свыше 300 высококвалифицированных специалистов, располагает 7 дочерними компаниями в Азербайджане, Эстонии, Грузии, Казахстане, Кыргызстане, Латвии, Узбекистане.

BS/2 ведёт свою деятельность в 80 странах мира, располагая более чем 800 международными клиентами и партнёрами во всём мире. В их числе:

- банковские и финансовые учреждения;
- предприятия розничной торговли;
- автозаправочные станции;
- почтовые службы;
- прочие компании (ипподромы, ломбарды, казино и др.).

ServiceDesk.iQ

Управление и оптимизация сервисного обслуживания

Service Desk .iQ
.iQ Family Product

Service Desk.iQ – решение для автоматизации процессов сервисного обслуживания оборудования для банков и предприятий розничной торговли, отвечающее за открытие, распределение, выполнение и закрытие клиентских заявок, организацию работы персонала сервисной компании и формирование отчетности.

Приложение 1. Глубокое обучение и свёрточные нейронные сети для защиты видеобезопасности

Один из вариантов трактовки термина «интеллект» (*intelligence*) состоит в его определении как «способности принимать правильные решения в соответствии с заданным критерием» (пример, способность выживание в мире животных).

Современные компьютеры уже обладают некоторым интеллектом благодаря программистам, создавшим для них программы. Поэтому компьютеры способны на действия, которые люди могут считать полезными (в этом случае говорят, что компьютер принял правильные решения). Тем не менее, обширное множество задач, с которыми животные и люди справляются довольно легко, всё ещё остаются вне досягаемости компьютеров. В качестве примера можно привести узнавание акцента говорящего человека или его лица по снимкам.

Для принятия более существенных решений требуются знания в форме, полезной для интерпретации сенсорных данных и применения этой информации.

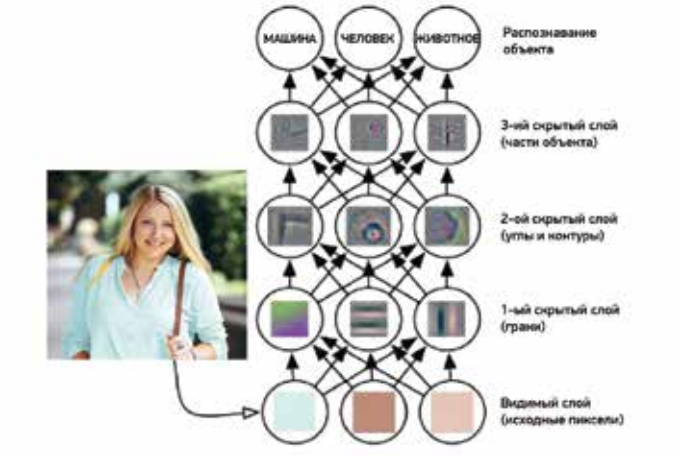
Многие из этих задач относятся к категории *«искусственный интеллект»* (*ИИ)* или *artificial intelligence (AI*) и включают в себя ряд задач восприятия и контроля.

Благодаря *ИИ* компьютеры способны учиться на опыте и понимать мир в терминах иерархии понятий – с каждой концепцией, определённой с точки зрения её отношения к более простым понятиям. Собирая знания из опыта, этот подход поможет избежать необходимости того, чтобы операторы (т.е., люди) формально определяли все знания, необходимые компьютеру для решения данной конкретной задачи.

Как добиться того, чтобы машины приобрели такой «искусственный интеллект»? Ответ состоит в использовании данных и примеров для создания эксплуатационных знаний – т.е., обучении машин.

Глубокое обучение (*deep learning*)— это специализированный вид машинного обучения, который учит компьютеры делать то, чем люди наделены от природы: т.е., *учиться на примерах*. В последнее время глубокое обучение находится в центре внимания благодаря точности получаемых результатов. Ранее подобные результаты были недостижимы. В глубоком обучении компьютерная модель учится выполнять задачи классификации непосредственно из изображений, текста или звуковых наборов.

Основой для этого является иерархия понятий, что позволяет формировать сложные концепции, строя их из более простых. На ил. 33 показана архитектура модели со многими слоями. По этой причине данный подход получил название «глубокое обучение» (*deep learning*) для ИИ.

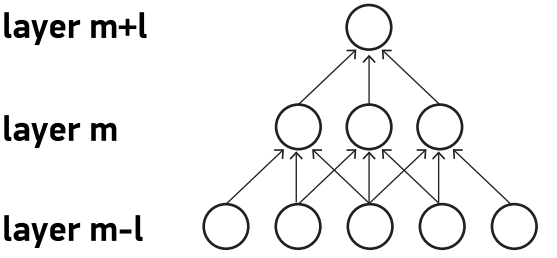


Ил. 33. Архитектура модели глубокого обучения.

Большинство методов глубокого обучения использует нейронные сетевые архитектуры.

Термин «глубокий» обычно относится к числу скрытых слоёв в нейронной сети. Традиционные нейронные сети содержат лишь 2-3 скрытых слоя, а в глубоких сетях их может быть до 150. Модели глубокого обучения используют большие наборы помеченных данных и нейронных сетевых архитектур, которые изучают функции непосредственно по данным **без необходимости выделения признаков**.

Свёрточные нейронные сети (англ. *convolutional neural networks; CNN*) используют пространственно-локальную корреляцию, применяя локальную схему соединения между нейронами соседних слоев. Иными словами, входы скрытых блоков в слое m соединены с подмножеством блоков в слое m-1, блоки которого имеют пространственно-смежные рецепторные поля (ил.34).

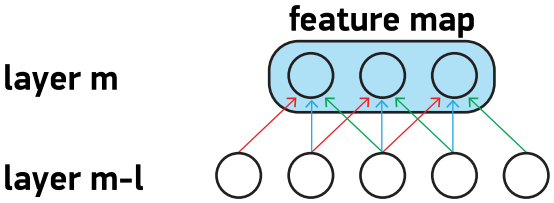


Ил. 34. Нейронные сети, организованные в слои, состоящие из набора взаимосвязанных узлов.

Такие сети могут иметь десятки или сотни скрытых слоев. Для наглядности представим себе, что слой m-1 является входной сетчаткой глаза (ил.34). Здесь блоки в слое m имеют рецепторные поля шириной 3 во входной сетчатке – и поэтому соединены только с 3 соседними нейронами в слое сетчатки. Блоки в слое m + 1 имеют такую же связность со слоем ниже. Считается, что ширина их рецепторного поля относительно слоя ниже также равна 3, однако ширина их рецепторного поля по отношению к входу больше, т.е., равна 5. Важно, что каждый из блоков не реагирует на изменения вне своего рецепторного поля

относительно сетчатки. Поэтому данная архитектура гарантирует, что обученные «фильтры» выдают наиболее мощный отклик на пространственно-локальный входной образ. При этом наличие такого многоуровневого множества слоёв приводит к нелинейным «фильтрам», которые становятся все более «глобальными» (т. е., реагирующими на большую область пространства пикселей). Например, устройство в скрытом слое m + 1 может кодировать нелинейную функцию ширины 5 (в терминах пространства пикселей).

Вдобавок к этому, в *CNN* каждый фильтр реплицируется по всему полю зрения. Эти реплицированные блоки используют одну и ту же параметризацию (вектор весов и смещение) и образуют карту признаков.



Ил. 35. Карта признаков для многослойной нейронной сети.

На ил. 35 показаны 3 скрытых блока, принадлежащих к одной и той же карте признаков. Веса одинакового цвета так разделены по блокам, чтобы быть одинаковыми в каждом из них.

CNN устраняют необходимость выделения признаков для классификации вручную, поэтому нет надобности выделять их для классификации изображений: *CNN* работает путём извлечения этих признаков непосредственно из изображений. Соответствующие признаки не требуют предварительного обучения – они выявляются нейронной сетью в ходе работы с набором изображений. Такое автоматическое извлечение признаков делает модели глубокого обучения весьма точными для задач компьютерного зрения – таких, как классификация объектов.

CNN учатся обнаруживать различные признаки изображения, используя десятки или сотни скрытых слоёв. Каждый скрытый слой увеличивает сложность усвоенных признаков изображения. Например, первый скрытый слой может узнать, как обнаружить края, а последний узнает, как обнаруживать более сложные формы, конкретно связанные с формой объекта, который следует распознать.

Отметим, что рабочий процесс машинного обучения начинается с того, что соответствующие признаки извлекаются вручную из изображений. Затем эти признаки используются для создания модели, которая классифицирует объекты на изображении.

Благодаря процессу глубокого обучения соответствующие признаки автоматически извлекаются из изображений. Кроме того, глубокое обучение выполняет «сквозное обучение» – в которых сети даются не обработанные данные и задача для решения (такая, как классификация), и сеть учится делать это автоматически.

Ключевым преимуществом сетей глубокого обучения является то, что их результаты часто продолжают улучшаться по мере увеличения размера входных данных.

В большинстве приложений глубокого обучения используется подход, основанный на передаче «опыта» (*transfer learning*): это процесс, включающий в себя тонкую настройку предварительно подготовленной модели.

С этой целью можно начать работу с имеющийся сети и загружать её новыми данными, содержащими неизвестные ранее классы. После внесения некоторых изменений в сеть можно выполнить новую задачу – такую, как выделение одних только людей или одних только банкоматов из разнообразных иных объектов на снимках. При этом преимуществом является то, что требуется гораздо меньший объём данных (т.е., нескольких тысяч, а не миллионов изображений), поэтому время вычисления сокращается до нескольких минут или часов.

В дополнение к распознаванию объектов, идентифицирующих конкретный объект на фото или видео, глубокое обучение также может быть использовано для их обнаружения. Таким образом глубокое обучение находит естественные применения для защиты и видеобезопасности в самых разных сферах деятельности.

Приложение 2. Глоссарий

Битрейт (англ. *bitrate*) – скорость передачи данных в единицах (битах), передаваемых за единицу времени (секундах). Измеряется в *Кбит/с* или *Мбит/с*.

Видеоаналитика (также *video analytics* или *video content analysis*) — направление, в рамках которого с помощью методов компьютерного анализа видеоконтента формируются результирующие данные о наблюдаемых объектах.

Видеокамера – устройство, преобразующее оптическое изображение наблюдаемого объекта в электрический видеосигнал. Видеокамеры делятся на проводные и беспроводные, по типу устройства входа – на аналоговые и цифровые.

Видеокамера купольная – наиболее распространенный вид камер со сферическим корпусом.

Видеосервер (англ. *video server*) — устройство (сервер), предназначенное для приёма, хранения, воспроизведения или ретрансляции видео- и/или аудиосигнала; обработки изображений.

CCTV камера – камера для наблюдения за периметром здания, на прилегающих к нему территориях и других уличных объектах.

IP-камера – стационарно установленная камера, имеющая встроенный *IP*-сервер, сетевой интерфейс и подключающаяся непосредственно к сети *LAN / WAN / Internet*.

Видеоквадратор – устройство, обеспечивающее размещение изображений от четырёх видеоисточников на одном экране, разделенном на четыре части (квадранта).

Видеокоммутатор – устройство для последовательного переключения видеосигналов от нескольких видеокамер на один или несколько выходов (мониторов).

Видеомультиплексор – система видеозаписи и управления с широкими функциональными возможностями для записи видеосигналов от нескольких (до 16) камер на одну видеокассету (кодирование), воспроизведение кодированных кассет и обработку сигналов тревоги.

Видеонаблюдение – процесс, осуществляемый с применением технических средств, служащий для визуального контроля за охраняемыми или наблюдаемыми объектами

Детектор движения – электронный блок или компьютерная программа, хранящая в памяти текущее изображение с телекамеры и подающая сигнал тревоги при возникновении изменений в зоне контроля.

ИК-камера – видеокамера с инфракрасной подсветкой (позволяет камере «видеть» в темноте)
Существуют проводные и беспроводные каналы передачи видеосигнала.

Кадр (англ. *frame*) — это единичное полное изображение. В формате чересстрочной развёртки 2:1 стандартов *RS-170* и *CCIR* кадр составляется из двух раздельных полей с 262,5 или 312,5 строками, чередующихся с частотой 60 или 50 Гц, что позволяет формировать полный кадр с частотой 30 или 25 Гц. В видеокамерах с функцией прогрессивной развёртки каждый кадр разворачивается построчно и не чередуется. Как правило, частота кадров составляет также 30 и 25 Гц.

Кодек *(англ. codec)* – программное обеспечение (ПО), осуществляющее преобразование аналогового сигнала в цифровую форму с последующим преобразованием цифрового сигнала, с тем, чтобы он мог быть передан по более узкополосным каналам связи.

В коммуникационной инженерии «кодек» обычно обозначает «кодер/декодер». Кодеки используются в интегральных микросхемах или чипах, конвертирующих аналоговые аудио- и видеосигналы в цифровой формат для последующей передачи. Кодек также преобразует полученные цифровые сигналы в аналоговый формат. Кодек сочетает функции преобразования аналогового сигнала в цифровой, и цифрового – в аналоговый в одной микросхеме.

Матричный видеокоммутатор – устройство для формирования нескольких последовательностей изображений от видеокамер в любом порядке с управлением их поворотными устройствами и вариообъективами, а также выводить номера камер и названия помещений, в которых они установлены, сообщения о сигналах тревоги, текущее время, дату, инструкции оператору и т.п.

Медиаконтейнер – файл для хранения цифровой информации и видео.

Пиксель (англ. *pixel*) – базовый дискретный элемент изображения.

Поворотная высокоскоростная камера – такая камера имеет значительно большую зону охвата, нежели стационарные видеокамеры, позволяя отслеживать одновременно несколько основных зон контроля.

Разрешение изображения — параметр, определяющий степень детальности цифрового изображения. Чем выше разрешение, тем выше уровень отображения деталей. Разрешение характеризуется отношением количества пикселей по горизонтали (ширина) к количеству пикселей по вертикали (высота), например, 320 x 240. Также для обозначения разрешения может использоваться общее количество пикселей.

Разрешающая способность – максимальное количество телевизионных линий, различаемых в выходном сигнале камеры при минимально допустимой глубине модуляции 10%.

Сетевой видеорегистратор (англ. *Network Video Recorder; NVR*) – предназначены для работы в IP-системах видеонаблюдения. В отличие от обычных цифровых видеорегистраторов (*Digital Video Recorder*; *DVR*) — устройства, предназначенного для записи, хранения и воспроизведения видеоинформации) *NVR* получают видеоданные уже в сжатом виде по сети *Ethernet*. Данные могут поступать с аналоговых или *IP*-видеокамер, подключаемых через специальные адаптеры (типа: «композитный сигнал — *Ethernet*»). Особенностью *NVR* является то, что они могут работать лишь с ограниченным списком моделей *IP*-видеокамер, поскольку в настоящее время стандартизация их интерфейсов сетевого обмена ещё не распространена.

Сетевой концентратор (англ. *hub*) — служит для подключения нескольких устройств к сети; осуществляет передачу всех

данных всем подключенным к нему устройствам – в то время, как коммутатор обеспечивает передачу данных только тому устройству, которому они предназначены.

Телекран (англ. *telecrane*) – вымышленное устройство для приёма и передачи видеосигнала, описанное в антиутопии Джорджа Оруэлла (настоящее имя Эрик Артур Блэйр (Eric Arthur Blair); 1903-1950) «1984».

Телевидение стандартной чёткости (*Standard Definition Television, SDTV*) – разновидность телевизионных вещательных стандартов, параметры которых выбраны, исходя из расстояния наблюдения, равного шести высотам наблюдаемого изображения. Системы стандартной чёткости основаны на стандартах разложения 625/50 (576i) и 525/60 (480i), существующих с 1940-х годов, когда телевидение стало массовым. Существуют аналоговое и цифровое телевидение стандартной чёткости, однако термин SDTV чаще всего применяется по отношению именно к цифровому телевидению. Характеризуется соотношением сторон 4:3 и обычным качеством.

Телевидение высокой чёткости (*High Definition Television; HDTV*; в России в официальных документах используется аббревиатура *ТВЧ*) — система телевидения с разрешающей способностью по вертикали и горизонтали, увеличенной примерно вдвое по сравнению со стандартной.

Тепловизор – прибор, который функционирует в тепловом (невидимом для человеческого глаза спектральном диапазоне), позволяя видеть то, что недоступно приборам ночного видения и видеокамерам.

Фокусное расстояние – расстояние между оптическим центром линзы объектива и фокальной плоскостью (ПЗС-матрицей) видеокамеры.

Формат CIF (англ. *Common Intermediate Format*) – базовый формат передачи видеоизображения, используемого в видеонаблюдении, зависящий от их разрешения.

Формат сжатия H.264 – стандарт сжатия видео, предназначенный для достижения высокой степени сжатия видеопотока при сохранении высокого качества.

Формат сжатия JPEG – алгоритм сжатия полноцветных неподвижных изображений. Изображение в формате *JPEG* — это растровое изображение с расширением .JPG или .JPEG. При создании изображения в формате JPEG можно задать уровень сжатия. Чем ниже уровень сжатия (и, соответственно, выше качество) изображения, тем больше размер файла.

Формат сжатия M-JPEG – покадровый метод видеосжатия, основной особенностью которого является сжатие каждого отдельного кадра видеопотока с помощью алгоритма сжатия изображений *JPEG*.

Формат сжатия Motion JPEG — технология сжатия и распаковки сетевого видеоматериала. Она обеспечивает низкую задержку и стабильное качество изображения независимо от его динамики и сложности. Качество изображения задается уровнем сжатия, который, в свою очередь, определяет размер файла и, таким образом, скорость передачи. Из видеопотока в формате *Motion JPEG* можно легко извлечь отдельные изображения высокого качества.

Формат сжатия MPEG-1 – группа стандартов на цифровое сжатие аудио и видео, принятая *Moving Picture Experts Group*.

Формат сжатия MPEG-2 – наименование группы стандартов цифрового кодирования видео- и аудиосигналов. Данный формат используется преимущественно для широкополосного

вещания, включая цифровое спутниковое и кабельное телевидение.

Формат сжатия MPEG-4 – международный стандарт, используемый преимущественно для сжатия цифрового аудио и видео. Основными областями применения стандарта *MPEG-4* являются Интернет (средства потоковой передачи данных), компакт-диски, средства коммуникации (видеотелефоны) и телевизионное вещание.

Частота кадров (англ. *framerate*) — это частота, с которой происходит обновление видеопотока; измеряется в кадрах в секунду.

Чересстрочная развёртка – метод формирования кадров, применяемый в телевидении.

Aspect ratio (форматное соотношение) – соотношение ширины изображения к его высоте. Стандартное форматное соотношение для телевизионных экранов и компьютерных мониторов — 4:3. В телевидении высокой чёткости (*HDTV*) используется формат 16:9.

AVI (Audio Video Interleave; чередование аудио и видео) – медиаконтейнер (формат), поддерживающий одновременное воспроизведение аудио и видео.

Bitmap (растровое изображение) – файл данных, представляющий собой прямоугольную расчётную сетку пикселей. Она определяет место и цвет каждого пикселя (или бита) на экране. Этот тип изображения также называется растровой графикой. Форматы *GIF* и *JPEG* являются примерами типов файлов, содержащих растровое изображение.

Client/server (клиент-сервер) – процесс, описывающий взаимодействие двух компьютерных программ, при котором

одна программа (клиент) направляет запрос к службе другой программе (серверу), которая должна выполнять этот запрос. Как правило, несколько клиентских программ обращаются к одной общей серверной программе.

CCTV (closed circuit television) – системы замкнутого телевидения, часто применяется как синоним термина "видеонаблюдение".

Coaxial cable (коаксиальный кабель) — стандартное средство передачи аналогового видеосигнала в замкнутых телевизионных системах. Также используется для бытового кабельного телевидения.

DSP (Digital Signal Processing) – цифровая обработка сигналов.

DV (Digital Video) – один из первых алгоритмов сжатия для видеопотока.

DVR (Digital Video Recorder) – цифровой видеорегистратор.

GIF (**Graphics Interchange Format**; формат обмена графическими данными)— один из наиболее распространённых форматов графических файлов. Существуют две версии этого формата: *87a* и *89a*. Версия *89a* поддерживает анимацию.

H.264 (или **MPEG-4 часть 10**) — стандарт сжатия нового поколения для цифрового видео, который обеспечивает более высокое, чем *Motion JPEG* или *MPEG-4*, разрешение видео с тем же битрейтом и пропускной способностью, или же качеством видео при низкой скорости передачи.

HTTP (**Hypertext Transfer Protocol**; протокол передачи гипертекста) — набор правил по обмену файлами (текстовыми, графическими, звуковыми, видео- и другими мультимедиа

файлами) в сети. Протокол HTTP является протоколом высшего уровня в семействе протоколов *TCP/IP*.

HTTPS (**Hypertext Transfer Protocol over SSL**) — протокол передачи гипертекста посредством безопасных соединений) — сетевой протокол, используемый браузерами и веб-серверами для шифровки и расшифровки запросов страниц, отправленных пользователями и страниц, возвращенных сервером. Обмен шифрованными данными осуществляется благодаря использованию сертификата *HTTPS* (выпускаемого организацией, отвечающей за сертификацию), который гарантирует подлинность сервера.

IEEE 802.11 – семейство стандартов для беспроводных сетей. Стандарт *802.11* поддерживает передачу данных со скоростью 1 или 2 Мбит/с в диапазоне 2,4 ГГц. Стандарт *IEEE 802.11b* поддерживает передачу данных со скоростью до 11 Мбит/с в диапазоне 2,4 ГГц, в то время как стандарт *802.11g* позволяет достигать скорости передачи до 54 Мбит/с в диапазоне 5 ГГц.

Протокол IP (англ. *Internet Protocol*) – обеспечивает доставку пакетов данных по заданному адресу. Поскольку протокол *IP* является протоколом без организации соединения, что означает отсутствие установленного соединения между конечными точками, пакеты могут отправляться по различным маршрутам, что требует их прибытия в место назначения в правильном порядке. После прибытия пакетов по месту назначения другой протокол — TCP (*TransmissionControlProtocol;* протокол управления передачей) – сортирует их в требуемом порядке.

IP-адрес — это адрес в *IP*-сети, используемый подключенными к ней компьютерами и устройствами. *IP*-адрес позволяет всем подключенным компьютерам и устройствам находить друг друга и обмениваться данными. Во избежание конфликтов каждый *IP*-адрес сети должен быть уникальным. *IP*-адрес может быть фиксированным, а может быть назначен динамически (и

автоматически) протоколом *DHCP*. *IP*-адрес состоит из четырех групп (четверок) десятичных цифр, разделенных точками, например, 123.36.43.15.

LAN (**Local Area Network**; локальная сеть) — это группа компьютеров и иных устройств, использующих одни и те же ресурсы и находящихся на ограниченной территории.

MPEG (**Moving Picture Experts Group**; группа экспертов по вопросам кинотехники) – разрабатывает стандарты сжатия цифрового видео и аудио; является подразделением Международной организации по стандартизации (*International Organization for Standardization; ISO*).

Multicast (многоадресная передача) – технология оптимизации использования полосы пропускания на основе одновременной доставки одного потока данных нескольким пользователям сети.

Multiplexer (мультиплексор) — высокоскоростной коммутатор, обеспечивающий одновременную передачу полноэкранных изображений с нескольких аналоговых видеокамер (до 16). Мультиплексор обеспечивает воспроизведение изображения с любой камеры без помех со стороны остальных камер системы.

NTSC (**National Television System Committee**; Национальный комитет по телевизионным системам) — это система аналоговой цветовой кодировки, используемая в телевещательных системах Японии, США и других стран американского континента. В системе *NTSC* каждый кадр видеосигнала состоит из 525 строк с частотой обновления 30 кадров в секунду.

PAL (**Phase Alternating Line**; строка с переменной фазой) — система аналоговой цветовой кодировки, используемая в телевещательных системах Европы и других стран мира. В

системе *PAL* каждый кадр видеосигнала состоит из 625 строк с частотой обновления 25 кадров в секунду.

Proxy server (прокси-сервер) – выступает в качестве посредника между пользователями рабочих станций и Интернетом, обеспечивая безопасность, администрирование и службы кэширования. Прокси-сервер, связанный с сервером шлюза или его частью, эффективно отделяет внутреннюю сеть предприятия от внешней сети и локального межсетевого экрана.

PTZ-камера – современная роботизированная камера видеонаблюдения, отличающаяся высокой скоростью изменения угла съёмки.

Server (сервер) — компьютерная программа, предоставляющая службы другим компьютерным программам на одном или нескольких компьютерах. Компьютер, на котором установлена серверная программа, также часто называют сервером. Сервер может содержать любое количество серверных и клиентских программ. Веб-сервер — это компьютерная программа, доставляющая запрашиваемые HTML-страницы или файлы клиенту (браузеру).

SNMP (**Simple Network Management Protocol**; простой протокол сетевого управления) – является частью пакета протоколов *IP* согласно постановлению рабочей группы «Инженерного совета Интернета» (*Internet Engineering Task Force;* IETF*)*. Данный протокол поддерживает наблюдение за устройствами, подключенными к сети, с целью оповещения администратора при возникновении каких-либо проблем.

SSL/TLS (**Secure Socket Layer / Transport Layer Security;** протокол защищённых сокетов / безопасность на транспортном уровне) – два протокола – *SS*L и *TLS* – являются криптографическими протоколами, обеспечивающими безопасный обмен данными в сети. Обычно протокол *SSL*

используется совместно с *HTTP*, в результате чего образуется протокол *HTTPS*, который часто применяется для электронных финансовых операций в Сети. Протокол *SSL* использует сертификаты открытого ключа для проверки подлинности серверов.

TCP (**Transmission Control Protocol**; протокол управления передачей) – используется вместе с протоколом *IP* для передачи пакетов данных между компьютерами в сети. В то время как протокол *IP* обеспечивает непосредственную доставку пакетов, *TCP* отслеживает путь отдельных пакетов, составляющих блок данных, и осуществляет их сборку в файл после доставки по месту назначения.

UDP (**User Datagram Protocol**; протокол дейтаграмм пользователя) — протокол обмена данными с ограничениями на пересылаемые данные по сети, использующей протокол *IP*. Протокол *UDP* является альтернативой протоколу *TCP*. Преимущество протокола *UDP* состоит в том, что для него необязательна доставка всех данных и некоторые пакеты могут быть пропущены, если сеть перегружена. Это особенно удобно при передаче видеоматериалов в режиме реального времени, поскольку не имеет смысла повторно передавать устаревшую информацию.

Unicast (одноадресная передача) – обмен данными между одним отправителем и одним получателем в сети. Для каждого нового пользователя устанавливается новое соединение.

Video surveillance as a service (VsaaS) – видеонаблюдение как сервис

Virtual Private Network (VPN) — виртуальная частная сеть. Позволяет создавать безопасные туннели между точками данной сети. В виртуальной частной сети могут работать лишь устройства, обладающие правильным «ключом».

VOP (Video Object Plane; объектная видеоплоскость) — это один кадр изображения в формате видеопотока *MPEG-4*. Существует несколько типов *VOP*. — *I-VOP* — это полный кадр изображения. — *A P-VOP* кодирует разницу между изображениями, до тех пор, пока это целесообразно. В противном случае он кодирует все изображение, которое также может быть совершенно другим изображением.

WAN (**Wide-Area-Network**; глобальная сеть) - сеть, аналогичная локальной, но большего географического масштаба.

Web Server (веб-сервер) — программа, позволяющая веб-браузерам получать файлы с компьютеров, подключенных к Интернету. Веб-сервер принимает запрос файла от веб-браузера и по его получении отправляет запрашиваемый файл браузеру. Основной функцией веб-сервера является предоставление страниц другим удаленным компьютерам, по этой причине он должен быть установлен на компьютере, постоянно подключенном к Интернету. Он также управляет доступом к серверу наряду с отслеживанием и ведением журнала статистики доступа к серверу.

WDR (**Wide Dynamic Range**; технология широкого динамического диапазона) – разница в освещённости между самой тёмной и самой светлой точками конкретного кадра; существенный контраст между яркими и тёмными областями.

Литература

[1.] Владо Дамьяновски. Библия видеонаблюдения, 3-е издание: Пер. с англ. – М.: Секьюрити Фокус, 2017. – 422 с.: ил. (Серия «Энциклопедия безопасности»)

[2]. У. Прэтт. Цифровая обработка изображений: Тт. 1- 2. Пер. с англ. - М.: Мир, 1982.

[3]. Richard O. Duda, Peter E. Hart and David G. Stork. Pattern Classication and Scene Analysis (2nd ed.), 1995

[4]. Торстен Анштедт, Иво Келлер, Харальд Лутц. Видеоаналитика: Мифы и реальность. – М., Секьюрити Фокус, 2012 - 174 с.

[5]. Джордж Оруэлл. «1984» и эссе разных лет. Пер. с англ. - М.: Прогресс, 1989.

[6]. *ATMeye.iQ*. http://www.atmeye.com/ru/o-produkte/

[7]. Рост рынка видеонаблюдения подпитывается обилием больших данных // Security News 12.01.2018. http://www.sec-news.ru/foreign/23589.htm#ixzz56zIohYGu

[8]. Tim A. Scally State of the Market: Video Surveillance 2018 https://www.sdmmag.com/articles/94822-state-of-the-market-video-surveillance-2018?v=preview

[9]. Top Video Surveillance Trends for 2017. By the IHS Markit video surveillance group, https://cdn.ihs.com/www/pdf/TEC-Video-Surveillance-Trends.pdf

[10]. Видеоаналитика_из_облака_на_базе_VisionLabs_LUNA. http://www.tadviser.ru/index.php/Продукт:Крок:_

[11]. OpenCV (Open Source Computer Vision Library), https://opencv.org/

[12]. Motion Analysis Systems, https://winanalyze.com/

[13]. Tango Concepts. https://developers.google.com/tango/overview/concepts

[14]. Milestone XProtect, https://www.videosurveillance.com/manufacturers/milestone.asp

[15]. 4 разработки, сделавшие *ATMeye.iQ* лучшим решением для видеобезопасности банкоматов в 2017 году. http://www.bs2.lt/ru/novosti-o-produktah/4-razrabotki-sdelavshie-atmeyeiq-luchshim-resheniem-dlya-videobezopasnosti-bankomatov-v-2017-godu/

[16]. 2017 ATM AND SELF-SERVICE SOFTWARE TRENDS. https://nmgprod.s3.amazonaws.com/media/filer_public/37/84/37842221-ce8f-4726-b55c-438901cf2fc0/kal_guide_2017_final.pdf

[17]. Jill Jaracz. Managing ATM Security: Layered Approaches for 21st Century Issues https://www.atmmarketplace.com/whitepapers/managing-atm-security-layered-approaches-for-21st-century-issues/

[18]. Mobile Protector. https://www.gemalto.com/financial/ebanking/sdk/mobile-protector

[19]. EAST publishes 1st ATM crime update of 2018. https://www.atmmarketplace.com/news/east-publishes-1st-atm-crime-update-of-2018/?utm_source=AMC&utm_medium=email&utm_campaign=Week+In+Review&utm_content=2018-03-09

[20]. Microsoft improves its AI face and image recognition tools. https://venturebeat.com/2018/03/01/microsoft-improves-its-ai-face-and-image-recognition-tools/

[21]. Bengio, Y.; Courville, A.; Vincent, P. (2013). "Representation Learning: A Review and New Perspectives". IEEE Transactions on Pattern Analysis and Machine Intelligence. 35 (8): 1798–1828. arXiv:1206.5538 . doi:10.1109/tpami.2013.50.

[22]. Schmidhuber, J. (2015). "Deep Learning in Neural Networks: An Overview". Neural Networks. 61: 85–117. arXiv:1404.7828 . doi:10.1016/j.neunet.2014.09.003. PMID 25462637.

[23]. Convolutional Neural Networks (LeNet). Convolutional Neural Networks (LeNet) - DeepLearning 0.1 documentation. DeepLearning 0.1. LISA Lab. http://deeplearning.net/tutorial/lenet.html

[24]. Convolutional Networks and Applications in Vision. Yann LeCun, Koray Kavukcuoglu and Cl´ement Farabet, Computer Science Department, Courant Institute of Mathematical Sciences, New York University

[25]. BS/2 receives 2nd Product of the Year award for ATMeye.iQ solution. https://www.atmmarketplace.com/news/bs2-receives-2nd-product-of-the-year-award-for-atmeyeiq-solution/?utm_source=Email_marketing&utm_campaign=emnaAMC12222017&cmp=1&utm_medium=html_email

[26]. Role of Video in Transforming Retail Banking and Wealth Management. Angus Hislop, David Morland https://www.cisco.com/c/dam/en_us/about/ac79/docs/fs/Video-in-Retail-Banking_IBSG_0418FINAL.pdf

[27]. Дадашев, Т.М., Паукштис, С.С. Горизонты телевидения нового столетия, Вильнюс, 2011.

[28]. Решения для управления сценариями платежей и лояльности. http://www.ashburn.eu/ru/produkty/paylo

[29]. Даниель Фуксон. Современные возможности видеомониторинга: что должна уметь «умная» система. Журнал «Расчеты и операционная работа в коммерческом банке», №2/2018, http://futurebanking.ru/reglamentbank/article/4993?access_key=ktg3ak

Тахмасиб Дадашев

В настоящее время доцент Московского физико-технического института (технического университета, Россия). Имеет ученую степень кандидата физико-математических наук.

Является автором более 40 научных статей и 6 книг по информационным технологиям, распознаванию образов и программированию. В их числе – «FrontPage 98», «Язык Java в действии. Microsoft Visual J++ 6», «Горизонты телевидения нового столетия».

С 1997 года работает в качестве главного редактора издания «Penki Kontinentai», специализирующемся на проблемах технологического развития банковской отрасли и сферы розничной торговли.

В 2005-2007 годах был приглашен в качестве научного эксперта проекта «Branch Optimizer», который был проведен компанией BS/2 совместно с корпорацией Wincor Nixdorf (Германия). Также принимал участие в ряде проектов компании BS/2, в том числе в проекте «ASOMIS».

ISBN 978-609-01-2608-0

2018