ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

СОВРЕМЕННЫЕ ПОДХОДЫ В ПОСТРОЕНИИ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ С ИНТЕГРИРОВАННЫМИ АЛГОРИТМАМИ ВИДЕОАНАЛИТИКИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Методические рекомендации

Воронеж
2023

УДК 621.397
ББК 32.940.2

Коллектив авторов: С.А. Гречаный, Д.Ю. Калков, Н.И. Меркулова, М.В. Таравков

Рецензенты: И.А. Домнин, заместитель начальника тыла ГУ МВД России по Воронежской области – начальник ЦИТСиЗИ, полковник внутренней службы;
Р.О. Лисянский, начальник ООВиЭИТСОиБ ФГКУ «УВО ВНГ России по Воронежской области», подполковник полиции

Современные подходы в построении систем видеонаблюдения с интегрированными алгоритмами видеоаналитики для обеспечения безопасности объектов информатизации: методические рекомендации [Электронный ресурс] / С.А. Гречаный, Д.Ю. Калков, М.В. Таравков, Н.И. Меркулова // Воронеж: Воронежский институт МВД России, 2023. – 56 с.

Методические рекомендации посвящены вопросам повышения эффективности анализа видеоизображений в системах видеонаблюдения в интересах повышения безопасности объектов информатизации, обусловленная увеличением объемов видеоинформации. Материалы издания представляют собой научно-теоретический анализ проблем, связанных с функционированием систем видеонаблюдения с интегрированными алгоритмами видеоаналитики для обеспечения безопасности объектов информатизации, в частности, объектов правоохранительных органов.

Издание предназначено для курсантов и слушателей образовательных организаций МВД России.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Для обеспечения безопасности объектов различного функционального назначения и масштаба используется широкий спектр технических средств и систем. Системы охранного телевидения являются неотъемлемой частью практически любой современной комплексной или интегрированной системы безопасности. Они позволяют осуществлять дистанционный визуальный контроль обстановки на охраняемом объекте, прием, обработку, хранение и воспроизведение визуальной и аудиоинформации. Изображение, формируемой системой, предназначено для анализа оператором с целью принятия оперативных решений. Как показывает практика, зачастую оператору приходится продолжительное время анализировать изображение с нескольких видеокамер, расположенных на разных мониторах. В процессе дежурства зрительный аппарат утомляется, внимание притупляется, а это в свою очередь приводит к снижению эффективности реагирования на события. В этом случае, существенно повысить эффективность функционирования системы охранного телевидения и обеспечения безопасности в целом позволяет использование в составе системы специализированного программного обеспечения для анализа видеоизображений.

Первые системы охранного телевидения с функцией анализа видеоизображений осуществляли данную функцию на аппаратном уровне и позволяли обнаруживать простейшие события, например, движение во всем кадре или в его части (ROI, от англ. Region Of Interest – регион интереса). Данная функция называется детектор движения (motion detector). Фактически данная задача решалась аналоговой камерой путем измерения уровня и скорости изменения сигнала от отдельных структурных элементов изображения (пискселей). Результатом являлось изменение состояния выходных цепей видеокамеры с высокоимпедансного на низкомпедансное и наоборот. Такие цепи называют цепями типа «сухой контакт» в связи с тем, что между ними и цепями электромагнитного реле прослеживается некоторая аналогия. Действительно электроды реле находятся в воздушной среде или в вакууме и имеют два состояния: замкнутое – низкое сопротивление контакта и разомкнутое – высокое сопротивление. К этим цепям могут подключаться слаботочные оповещатели (световые, звуковые, комбинированные) или шлейфы сигнализации приемно-контрольных приборов. В дальнейшем такая функция появилась и у видеорегистраторов.

Повышение требований к эффективности обеспечения безопасности объектов в условиях воздействия различных угроз повлекло за собой появление новых функциональных возможностей и повышение технических характеристик систем охранного телевидения. Это стало возможным, в том числе, благодаря развитию электронных

вычислительных машин, появлению высокопроизводительных серверов, хранилищ данных и видеоадаптеров. Задачи, которые раньше решались на аппаратном уровне стали решаться программными средствами. Появилось понятие «видеоаналитика», которой в соответствии с ГОСТ 51558-2014 называется программное обеспечение, реализующее алгоритмы автоматизированного получения различных данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей.

Видеоаналитика начала свое развитие с обнаружения таких событий как пересечение линии, появление объекта в заданном секторе, детекция оставленных и пропавших предметов, движение в кадре с сопровождением.

Возможности современной видеоаналитики существенно расширились не только за счет развития средств вычислительной техники, но и за счет совершенствования математического аппарата описания и обработки видеоизображений, а также самого программного обеспечения. Для решения сложных, нестандартных задач стали применяться нейронные сети, которые являются математическими моделями, построенными по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма. К числу уже существующих функций видеоаналитики добавились распознавание лиц, толпы, драки, человека с оружием, заложников и др. Высокая эффективность систем видеонаблюдения с интегрированными алгоритмами видеоаналитики подчеркивает их актуальность и необходимость широкого применения на объектах различных категорий, в том числе объектах информатизации органов внутренних дел.

ГЛАВА 1. АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ И ОСОБЕННОСТЕЙ ДЕЯТЕЛЬНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

1.1. Обзор законодательной базы, регламентирующей деятельность объектов информатизации органов внутренних дел

Правовое обеспечение процессов информатизации представляет собой совокупность нормативных правовых актов, принимаемых на различных уровнях власти и управления, регулирующих комплекс общественных отношений, связанных с созданием и использованием информации и перспективных информационных технологий.

Правовой основой реализации Министерством своих полномочий в установленной сфере являются Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральный закон от 7 февраля 2011 г. №3-ФЗ «О полиции», Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Указ Президента Российской Федерации от 1 марта 2011 г. № 248 «Вопросы Министерства внутренних дел Российской Федерации», Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», а также нормативные правовые акты МВД России, регулирующие вопросы развития информационных технологий, связи и защиты информации.

Во исполнение перечня поручений Президента Российской Федерации от 9 августа 2011 г. № Пр-2291 разработана Концепция создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах, в соответствии с которой, на базе единой информационно-телекоммуникационной системы ОВД Российской Федерации, создавалась единая система информационно-аналитического обеспечения деятельности МВД России.

В целях обеспечения надлежащей реализации полицейских функций, автоматизации служебной деятельности ОВД и предоставления государственных услуг, в составе ИСОД МВД России созданы и внедрены общесистемные (СЭД, СУДИС, СЭП, ВИСП, СВКС-м, Форум, АПК «Официальный интернет-сайт МВД России») и прикладные сервисы (СООП, СОМТО; ФИС ГИБДД-М, СЦУО, ЦИАДИС, СОДИ, СПГУ, СОПС, СОДЧ, СОКД, СОШП, СОДПП, СФП, Ксенон-2).

Обеспечена возможность защищенного доступа к сервисам ИСОД МВД России посредством проводных, спутниковых и беспроводных каналов связи. Назначены администраторы доступа к Системе и организован процесс получения единых учетных записей пользователей ИСОД МВД России, количество которых ежегодно увеличивается.

В условиях формирования информационного общества в России конституционное закрепление информационных прав имеет большое политическое и юридическое значение. Конституция Российской Федерации закрепляет основные, базовые положения для всех отраслей права. Она содержит основополагающие нормы и в отношении информации. В Основном законе информации посвящено несколько статей (ст. 24, 29, 42, 71).

Ст. 24: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом».

Ст. 29 гласит: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (п. 4); «гарантируется свобода массовой информации. Цензура запрещается» (п. 5). Конституционные положения, закрепляющие основные информационные права и свободы, развиваются и детализируются в федеральном законодательстве. Рассматривая уровень федеральных законов, следует выделить следующие:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применение информационных технологий, обеспечение защиты информации);

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (регулирует отношения, связанные с обработкой государственными органами власти, юридическими и физическими лицами персональных данных, которые не составляют государственную тайну);

– Гражданский кодекс Российской Федерации (осуществляет правовое регулирование создания и использования программ для ЭВМ и баз данных: ст. 1261, 1262, 1280, 1333, 1334, 1335, 1336);

– Кодекс Российской Федерации об административных правонарушениях (закрепляет ответственность за нарушение норм в сфере обработки персональных данных: ст. 5.39, 13.11, 13.12, 13.14);

– Уголовный кодекс Российской Федерации (содержит статьи, определяющие ответственность за неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети и др. – ст. 137, 140, 272, 273, 274, 284, 292, 324);

– Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне» (регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ, определяет полномочия государственных органов и должностных лиц по обеспечению сохранности и защиты государственной тайны, содержит перечень сведений, составляющих государственную тайну);

– Федеральный закон от 09 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (регулирует отношения, связанные с обеспечением доступа пользователей информацией к сведениям о деятельности государственных органов и органов местного самоуправления, определены принципы и способы обеспечения доступа к информации, формы ее предоставления, права и обязанности пользователей информации, органов власти, их должностных лиц, установлена ответственность за нарушение порядка доступа к информации).

В рамках реформирования системы МВД России, понимая необходимость и важность правового урегулирования информационных отношений, возникающих в сфере внутренних дел, впервые на законодательном уровне был закреплен порядок применения информационных технологий и осуществления процесса защиты информации в ОВД:

– Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции». Пункт 3 ст. 8 данного закона обязывает сотрудников ОМВД регулярно информировать государственные и муниципальные органы, граждан о своей деятельности через средства массовой информации, информационно-телекоммуникационную сеть Интернет.

В информировании общественности большая роль принадлежит официальным сайтам территориальных органов МВД России. Разделы и рубрики ведомственных Интернет-ресурсов должны быть наполнены качественной и актуальной информацией, а также материалами, которые могут помочь гражданам в решении имеющихся вопросов;

– Указ Президента РФ от 01.03.2011 г. № 248 «Вопросы МВД РФ» вместе с Положением о МВД РФ в ред. от 24.10.2018 (утвердил Положение о МВД России, в котором указано, что Министерство формирует и ведет, в соответствии с законодательством Российской Федерации, федеральные учеты, базы данных оперативно-справочной, розыскной,

криминалистической, статистической и иной информации, а также использует в установленном порядке федеральные учеты, базы данных в этой области других федеральных органов исполнительной власти);

– Указ Президента РФ от 9 мая 2017 г. № 203 «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы»;

– Постановление Правительства РФ от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» (установило требования по обеспечению защиты информации, содержащейся в информационных системах общего пользования);

– Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (определяет для государственных и муниципальных органов, обрабатывающих персональные данные, необходимость обязательного принятия ряда документов, обеспечивающих выполнение законодательства в области персональных данных);

– Постановление Правительства РФ от 25 апреля 2012 г. № 394 «О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов» (скорректированы акты Правительства РФ по вопросам совершенствования использования информационно-коммуникационных технологий в деятельности государственных органов);

– Постановление Правительства РФ от 6 сентября 2012 г. № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти» (принят ряд мер по совершенствованию электронного документооборота в органах государственной власти, а также установлен срок (до 31 декабря 2017 г.) перехода к электронному взаимодействию федеральных органов исполнительной власти между собой и с Правительством РФ).

– Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (пересмотрены требования по защите этих данных при их обработке в соответствующих информационных системах. За безопасность персональных данных отвечает оператор системы, который их обрабатывает, или уполномоченное им лицо. Оператор системы выбирает средства защиты информации в соответствии с нормативными актами ФСБ России и ФСТЭК России).

– Постановление Правительства РФ от 25 декабря 2014 г. № 1494 «Об утверждении правил обмена документами в электронном виде при организации информационного взаимодействия» (определило правила обмена документами в электронном виде).

1.2. Основные направления деятельности объектов информатизации органов внутренних дел на примере структурных подразделений ГИАЦ МВД России

Основные направления деятельности федерального казенного учреждения «Главный информационно-аналитический центр Министерства внутренних дел Российской Федерации» состоят в следующем:

– централизованное информационное обеспечение в установленном порядке подразделений МВД России, органов государственной власти Российской Федерации, органов местного самоуправления, компетентных органов иных государств оперативно-справочными, оперативными, разыскными, криминалистическими, дактилоскопическими, статистическими, архивными сведениями, сведениями, содержащимися в информационных системах и банках данных в сфере миграции;

– формирование и ведение централизованных учетов, баз данных оперативно-справочной, разыскной, криминалистической, дактилоскопической, статистической и иной информации;

– формирование архивных фондов, осуществление учета, хранения, экспертизы научной и практической ценности, научно-технической обработки архивных документов, образовавшихся в деятельности служб центрального аппарата МВД (МООП) СССР, МВД (МООП) РСФСР, МВД СССР, МВД России и территориальных органов Министерства внутренних дел Российской Федерации;

– оказание услуг в целях обеспечения реализации предусмотренных законодательством Российской Федерации полномочий МВД России;

– обеспечение эксплуатации единой системы информационно-аналитического обеспечения деятельности МВД России;

– обеспечение эксплуатации и технической поддержки информационных систем и банков данных в сфере миграции.

Для достижения указанных целей Учреждение осуществляет для МВД России и находящихся в его ведении учреждений за счет средств федерального бюджета следующие виды деятельности:

– сбор, накопление статистической информации о состоянии преступности и результатах оперативно-служебной деятельности территориальных органов МВД России, оперативно-справочной, оперативной, розыскной, криминалистической, дактилоскопической,

архивной, научно-технической и иной информации с использованием средств вычислительной техники, телекоммуникационных и шифровальных (криптографических) средств;

– обработку и выдачу в установленном порядке для руководства Министерства, подразделений и учреждений МВД России, органов государственной власти Российской Федерации, а также правоохранительных органов иных государств запрашиваемой информации из учетов, баз и банков данных информационных систем, автоматизированных банков данных специализированных учетов, Межгосударственного информационного банка («МИБ»);

– формирование и ведение в порядке, установленном нормативными правовыми актами МВД России, учета документов и дел, образующихся в процессе оперативно-розыскной деятельности оперативных подразделений органов внутренних дел и Федеральной службы исполнения наказаний, а также документов и дел на лиц, в отношении которых заведены дела оперативного учета;

– обеспечение защиты персональных данных, содержащихся в информационных системах и базах данных ФКУ «ГИАЦ МВД России», в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– администрирование и техническое обслуживание средств удаленного доступа и локально-вычислительных сетей ФКУ «ГИАЦ МВД России» для обеспечения доступа сотрудников подразделений МВД России и территориальных органов МВД России, других правоохранительных органов Российской Федерации и СНГ к информационным ресурсам ФКУ «ГИАЦ МВД России»;

– подготовку и выпуск малотиражных изданий, изданий в электронном виде о состоянии оперативно-служебной деятельности органов внутренних дел, обзорных информационно-аналитических материалов, в том числе с использованием в установленном порядке специальных информационных систем ФСО России;

– участие в пределах компетенции совместно с подразделениями МВД России мероприятий по стандартизации учетно-регистрационных документов, разработке проектов форм государственной и ведомственной статистической отчетности о состоянии преступности и результатах оперативно-служебной деятельности органов внутренних дел;

– осуществление организационно-методического руководства деятельности информационных центров территориальных органов МВД России.

Учреждение в установленном порядке и в пределах своей компетенции вправе осуществлять следующие виды приносящей доход деятельности по договорам с юридическими и физическими лицами:

– выполнение мероприятий по аттестации объектов информатизации, обрабатывающих сведения, составляющие государственную тайну, служебную информацию и персональные данные, по требованиям безопасности в соответствии с нормативными правовыми документами ФСТЭК и ФСБ России, на основании выданной в установленном порядке лицензии;

– полиграфическая деятельность и реализация печатной продукции по вопросам деятельности Учреждения;

– оказание информационных и консультационных услуг в установленной сфере деятельности в порядке, предусмотренном законодательством Российской Федерации, межведомственными и межправительственными соглашениями.

В свою очередь, информационные центры в системе органов внутренних дел в регионах являются головной организацией в областях:

– обеспечения статистической, оперативно-справочной, разыскной, криминалистической, архивной и научно-технической информацией;

– планирования, координации и контроля процессов создания, внедрения, использования, развития современных информационных технологий, автоматизированных информационных систем общего пользования и интегрированных банков данных общего пользования, средств вычислительной техники и системного программного обеспечения к ним.

Обеспечение руководства, подразделений ГУ, органов внутренних дел, органов государственной власти субъекта РФ статистической информацией о состоянии преступности и результатах оперативно-служебной деятельности органов внутренних дел, оперативно-справочной, разыскной, криминалистической, архивной и иной информацией в порядке, установленном нормативными правовыми документами МВД России.

Формирование в Главном управлении единой системы статистических, оперативно-справочных, разыскных и криминалистических учетов.

Проведение единой научно-технической политики в рамках развития информационно-вычислительной системы ГУ на основе нормативных документов ФКУ «ГИАЦ МВД России».

Обеспечение исполнения в органах внутренних дел субъектов Российской Федерации основ законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах в части, относящейся к документам Архивного фонда Российской Федерации, находящимся на хранении и образующимся в органах внутренних дел, а также законодательства Российской Федерации о реабилитации граждан, подвергшихся политическим репрессиям в административном порядке.

1.3. Каналы утечки информации на объектах информатизации органов внутренних дел

Повышенные требования к обеспечению информационной безопасности предъявляет нынешний уровень и темпы технического прогресса. За последние годы количество физических процессов и объектов, используемых информационными технологиями, многократно увеличилось. И появление в информационной сфере каждого нового технического и технологического процесса вызывает новые специфические требования к защите информации. Под защитой информации в соответствии с Федеральным законом № 149-ФЗ понимается принятие правовых, организационных и технических мер, направленных: – на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; – на соблюдение конфиденциальности информации ограниченного доступа; – на реализацию права на доступ к информации. Под техническим каналом утечки информации принято понимать систему, в состав которой входят:

1) объект разведки;

2) техническое средство, используемое для несанкционированного получения сведений;

3) физическая среда, в которой распространяется информационный сигнал.

Объектом разведки могут быть помещение, группа помещений или здание с хранящимися материалами ограниченного пользования, технические каналы связи, используемые для передачи сведений, отнесенных к различным видам тайн. Физической средой, в которой распространяются информационные сигналы, могут быть строительные конструкции зданий и сооружений, токопроводящие линии, среда распространения акустических (речевых) сигналов, электромагнитные поля.

Средой распространения информации на объектах информатизации являются также технические средства обработки информации (далее – ТСОИ), находящиеся в помещении, – средства вычислительной техники, автоматические телефонные станции, системы звукозаписи.

Выделим следующие группы основных технических каналов утечки информации:

1) электромагнитные;

2) электрические;

3) каналы утечки видовой информации;

4) каналы утечки акустической (речевой) информации.

Заметим, что это неполный перечень всех возможных технических каналов утечки информации и методов ее несанкционированного перехвата. Электромагнитные каналы утечки информации. Вся работающая электронная аппаратура и электронные системы, на какой бы технической базе они ни создавались, от телефонного аппарата до современных компьютерных систем, от релейно-контактных и электронно-вакуумных модулей до сверхбольших интегральных схем и проводных коммуникаций создают электромагнитные поля, называемые побочными электромагнитными излучениями. Они способны создавать электромагнитные наводки в расположенных рядом слаботочных, силовых и осветительных сетях, линиях и аппаратуре охранно-пожарной сигнализации, проводных линиях связи, различных приемниках электромагнитных излучений. В результате таких процессов возникают каналы утечки информационных сигналов, т. к. электромагнитное поле, создаваемое работающей аппаратурой, является носителем обрабатываемой или передаваемой информации. Специальные широкополосные приемники позволяют «считывать» электромагнитные излучения, а затем восстанавливать и отображать содержащуюся в них информационную составляющую.

Электрические каналы утечки информации возникают за счет:

– наводок электромагнитных излучений ТСОИ на коммутационные линии вспомогательных технических систем и средств (далее – ВТСС);

– утечек информационных сигналов в цепях электропитания ТСОИ;

– утечек информационных сигналов в цепь заземления ТСОИ.

Например, побочные электромагнитные поля работающих компьютеров производят наводки на близко расположенные коммутационные линии ВТСС (охранно-пожарная сигнализация, телефонные провода, сети электропитания, металлические трубопроводы).

Наводимая в них ЭДС существенна и распознаваема на частотах от десятков кГц до десятков мГц. В этом случае возможен съем информации путем подключения специальной аппаратуры к коммуникационным линиям за пределами контролируемой территории. Каналы утечки видовой информации.

Несанкционированное получение видовой или, как ее иногда называют, графической информации осуществляют путем наблюдения за объектом, представляющим оперативный интерес. Различных видов технических средств, используемых для этих целей, достаточно много – это бинокли, приборы ночного видения, фото- и видеотехника, и др. Каналы утечки акустической (речевой) информации. Наиболее распространенным способом несанкционированного доступа к информации является перехват акустической (речевой) информации.

Каналы утечки акустической (речевой) информации принято классифицировать следующим образом:

– электроакустический;
– виброакустический;
– оптико-электронный;
– акустический;
– проводной;
– электромагнитный.

Ряд элементов ВТСС, прежде всего, громкоговорители трансляционной сети, звонки телефонных аппаратов меняют свои электрические параметры (емкость, индуктивность, сопротивление) под действием акустического сигнала. Изменение названных параметров вызывает модуляцию информационным сигналом токов, протекающих в элементах ВТСС. Такие электроакустические преобразования получили название «микрофонного эффекта». С точки зрения безопасности, телефонный аппарат имеет существенный недостаток, поскольку его основные узлы (микрофон, мембрана, звонковая цепь) могут выполнять функции приемника и передатчика сигналов при несанкционированном прослушивании помещения, в котором он установлен. Звонковая цепь телефонного аппарата при положенной на рычаг трубке обладает «микрофонным эффектом». Подвижные части звонка вибрируют под действием речевых сигналов (разговор в помещении), что приводит к появлению в нем электрического тока малой амплитуды. Это, в свою очередь, позволяет провести соответствующую обработку возникающего в цепи сигнала и выделить звуковую составляющую за пределами контролируемого помещения.

. В результате снятия результатов воздействия акустических речевых сигналов на строительные конструкции и сооружения (панели перегородок стен, пол, потолок, воздуховоды, вентиляционные шахты, трубы и батареи отопления, оконные стекла и т. д.) возникает виброакустический канал несанкционированного снятия информации из контролируемых помещений. Под воздействием акустических волн строительные конструкции подвергаются микродеформации, в результате которой возникают упругие механические колебания, хорошо передающиеся в твердых однородных средах. Эти колебания воздействуют на чувствительный элемент электронного стетоскопа (вибродатчик) и преобразуются в электрический сигнал, который затем усиливается и может быть передан по проводным, оптическим или радиоканалам связи. Оптико-электронный канал утечки информации. Акустический контроль удаленных помещений, имеющих окна, может быть осуществлен с использованием оптико-электронных или, как их нередко называют, лазерных систем (лазерных микрофонов). Современные лазерные системы позволяют осуществлять прослушивание разговоров, ведущихся в помещении, на расстоянии от 100 м до 1 км. Дальность действия во многом зависит от качества оконного стекла (величины

микронеровностей), а также от степени его загрязненности и состояния атмосферной среды (от метеоусловий, задымленности и др.). С улучшением отражающей поверхности увеличивается дальность действия. Для этого применяются следующие приемы: стекло покрывается специальным материалом либо на нем наклеиваются небольшие отражатели. Для отражения лазерного луча могут быть также использованы элементы интерьера и мебели – стеклянные поверхности и зеркала внутри помещения.

Самым простым способом перехвата речевой информации, не требующим использования специальной техники, является подслушивание ведущихся разговоров. Неплотно прикрытая дверь в кабинет должностного лица, обсуждение сведений ограниченного распространения в курительной комнате или за пределами служебных помещений, конфиденциальное совещание, проводимое в помещении с открытыми окнами, – вот те простые, но вместе с тем вполне реальные каналы утечки информации. Проводные каналы утечки акустической (речевой) информации. В зданиях и сооружениях акустические каналы возникают как за счет имеющихся воздуховодов, вентиляционных шахт, некачественного строительства, так и за счет специально сделанных отверстий в потолках, стенах, полах. В этом случае для снятия акустической информации могут быть использованы проводные микрофоны, которые через линии связи подключаются к звукоусилительной и звукозаписывающей аппаратуре. В открытой периодике упоминается система акустического мониторинга с передачей команд управления и информации от нескольких микрофонных и телефонных входов по одной двухпроводной физической линии. Электромагнитные каналы утечки акустической (речевой) информации. Наряду с направленными микрофонами, диктофонами и лазерными системами, для несанкционированного съема речевой информации широко используются скрытно установленные акустические закладные устройства или, как их кратко называют, радиомикрофоны.

1.4. Средства и методы обеспечения информационной безопасности на объектах информатизации

Немаловажным фактором в защите информации, циркулирующей в информационной инфраструктуре ОВД, является ее защита от несанкционированного снятия со строительных конструкций зданий и сооружений служебных помещений. Развитие средств и систем несанкционированного снятия информации, открытость и относительная доступность их приобретения и изготовления ставят задачи по организации технической защиты на объектах ОВД, устойчивой к потенциальным угрозам несанкционированного снятия. Устранение акустических и виброакустических каналов утечки информации основано

на тех же физических процессах и явлениях, которые лежат в основе построения средств и методов несанкционированного снятия информации по акустическим и виброакустическим каналам – процессах распространения акустических волн в воздушных средах и распространения упругих волн в однородных средах, какими являются строительные конструкции служебных зданий и сооружений ОВД, а также коммуникации водоснабжения и отопления.

Так, защита от акустического снятия информации предполагает использование двух подходов. Первый основан на построении в служебных помещениях т. н. акустических демпферов – метод пассивной акустической изоляции. Второй метод предполагает активное акустическое и виброакустическое зашумление с помощью специальных генераторов низкочастотных (звуковых) шумовых акустических и виброакустических сигналов, которые предназначены для акустического и виброакустического зашумления каналов утечки информации. Защита от прямого акустического снятия информации основывается на выявлении и устранении строительных дефектов и изъянов с точки зрения ухудшения звукоизоляции: заделываются щели в стенах и перекрытиях, устанавливается дополнительная звукоизоляция в виде фальшпотолков, фальшстен, акустических и виброакустических экранов, акустических экранов водоотопительной системы, специальных оконных рам и вакуумного застекления. Кроме того, для зашумления воздуховодов, помещений небольшого объема (салон автомобиля, комнаты переговоров и т. д.), а также создания заградительных шумовых помех от снятия речевых сигналов направленными микрофонами используются устройства активного акустического зашумления. Для защиты речевых сигналов от несанкционированного снятия по виброакустическим каналам утечки информации используется метод активного виброакустического зашумления. Этот метод состоит в наведении в строительных конструкциях служебных зданий и сооружений упругих шумовых виброколебаний, которые распространяются по всему объему строительной конструкций, вызывая шумовые микродеформации, которые в свою очередь подавляют микродеформации, создаваемые воздействием речевых сигналов на те же конструкции, т. е. происходит шумовое виброзашумление упругих волн, создаваемых речевыми сигналами людей, находящихся в контролируемой зоне. В этом случае значительно снижается возможность, как восприятия речевых сигналов, так и их распознавания устройствами несанкционированного съема. Система виброакустического зашумления состоит из генератора низкочастотных шумовых сигналов, нескольких вибропреобразователей, осуществляющих формирование виброакустических сигналов. Датчики вибропреобразователей виброакустического зашумления в случае стационарного оборудования объекта защиты монтируются на

перекрытиях, стенах, водопроводных коммуникациях и отопительных батареях, вентиляционных шахтах, оконных переплетах и т. д., и создают заградительную виброакустическую помеху в элементах строительных конструкций. Во время отсутствия в контролируемых помещениях звуковых сигналов вибродатчики находятся в режиме «молчания», при появлении в контролируемых помещениях звуковых сигналов акустические микрофоны воспринимают их и вырабатывают команду для включения шумовых вибропреобразователей. В качестве перспективных разработок систем виброакустического зашумления выбрано направление на построение адаптивных систем, которые вырабатывают шумовую помеху в зависимости от материала и толщины строительных конструкций, определена тенденция на уменьшение габарито-весовых показателей. Такие системы позволяют автоматически оценивать результат виброакустического зашумления и выдавать данные о выполнении поставленной задачи. Результаты такого анализа сопровождаются в виде голосового сообщения.

Наиболее опасными с точки зрения несанкционированного снятия информации за счет побочных электромагнитных излучений и наводок (далее – ПЭМИН) являются мониторы компьютеров со стандартами разверток телевизионных систем. Во всех указанных случаях даже использование мощных криптографических средств и методов защиты не приводит к желаемым результатам, и только применение специальных методов и аппаратуры защиты от ПЭМИН способно устранить возникший канал утечки информации. Активное радиотехническое подавление и маскировка ПЭМИН заключаются в формировании и излучении в непосредственной близости от устройств вычислительной техники широкополосного шумового сигнала с уровнем излучения, превышающим уровень излучения информационного сигнала во всем частотном диапазоне, где имеются эти излучения, а также в осуществлении наводок, подавляющих побочные электромагнитные излучения, создаваемые информационными сигналами, в отходящие цепи коммутации и линии электропитания. Для осуществления электромагнитного подавления ПЭМИН разработан класс генераторов электромагнитных колебаний «белого электромагнитного шума», создающих шумовое электромагнитное поле в диапазоне частот от десятков килогерц до единиц и десятков гигагерц со спектральным уровнем излучаемого сигнала, существенно превышающим уровни электромагнитных излучений, создаваемых средствами вычислительной техники.

Существует два типа изделий электромагнитного зашумления:

1. Генераторы объемного электромагнитного зашумления.

2. Генераторы локального электромагнитного зашумления. Средства телефонной связи достаточно часто используются для несанкционированного получения информации, как конкурентами, так и

криминальными структурами, этому в немалой степени способствует отсутствие элементарного порядка в телефонном хозяйстве городов, предприятий и организаций.

Структурные методы защиты речевых сообщений с использованием телефонных линий связи и слаботочной аппаратуры можно классифицировать по следующим направлениям:

– обнаружение несанкционированного подключения устройств снятия речевых сигналов и активная защита телефонных линий;

– скремблирование речевых сигналов;

– шифрование речевых сигналов.

Наиболее вероятными каналами утечки речевой информации являются телефонные линии связи. Устройства активной защиты предназначены для нейтрализации несанкционированно-подключаемых устройств на участке «абонентский аппарат – телефонная станция». В этом случае нейтрализация устройств несанкционированного снятия осуществляется путем генерации в телефонную сеть низкочастотных и высокочастотных помех, а также управлением потребления тока в линии связи при ведении разговоров, что приводит к снижению соотношения сигнал/шум на входе несанкционированно подключенных устройств снятия речевых сигналов и блокировке акустопуска звукозаписывающей аппаратуры. То есть полезный сигнал на входе устройства снятия по отношению к специально создаваемой шумовой помехе становится такой величины, что несанкционированно подключенное устройство не срабатывает. Это исключает или уменьшает вероятность приема и распознавания полезного речевого сигнала.

Для активной защиты телефонных линий применяются следующие методы:

– блокирование (нейтрализация) устройств несанкционированного снятия за счет снижения отношения сигнал/шум на входе подслушивающего устройства;

– размывание спектра радиопередающего подслушивающего устройства;

– сдвиг рабочей частоты радиопередающего устройства в более высокочастотный диапазон, что приводит к невозможности восприятия и распознавания информационных сигналов приемниками несанкционированных пользователей;

– блокирование акустопуска звукозаписывающей аппаратуры;

– защита телефонного тракта от ВЧ-навязывания;

– осуществление гальванической развязки телефонного аппарата от линии связи за счет оптоэлектронных преобразователей;

– полное подавление устройств несанкционированного снятия специальными генераторами;

– методы скремблирования и шифрования телефонных переговоров.

В качестве активных методов защиты речевых сообщений в системах конфиденциальной связи нашли широкое применение различного рода скремблирующие устройства и устройства шифрования речевых сигналов.

Методы защиты речевых сообщений по степени стойкости к несанкционированному воздействию подразделяются:

– на методы обеспечения временной стойкости речевых сообщений от несанкционированного доступа;

– на методы гарантированной защиты информации от несанкционированного доступа.

К способам обеспечения временной стойкости речевых сообщений от несанкционированного доступа относят методы аналогового скремблирования, которые обеспечивают временную стойкость передаваемых сообщений за счет изменения характеристик исходного речевого сигнала таким образом, что выходной преобразованный речевой сигнал становится неразборчивым для несанкционированного пользователя. Преимуществом такого метода защиты речевых сообщений является относительная простота технической реализации, что определяет относительно низкую стоимость и малые габариты, возможность передачи заскремблированных сигналов по стандартным телефонным каналам и хорошее качество восстановления исходного речевого сигнала приемником при дескремблировании. Рассмотренные методы защиты информации в комплексном применении способны обеспечить надежную защиту информации, циркулирующей в информационных инфраструктурах ОВД, и создать надежный заслон несанкционированному восприятию и распознаванию сообщений со стороны несанкционированных пользователей.

Таким образом, можно заключить, что разработка практических рекомендаций по проведению мероприятий, направленных на достижение требуемого уровня защиты информации, возможна лишь после всестороннего изучения объекта защиты. Кроме того, необходимо получить достоверные оценки уровня защищенности циркулирующей в нем информации, определить, каким путем может быть организован несанкционированный съем информации, и обоснованно выявить вероятные каналы ее утечки. Утечки могут быть связаны с работой персонала, имеющего непосредственный контакт с циркулирующей информацией (например, сотрудники, обслуживающие программно-аппаратные средства вычислительной техники). Причем эти утечки могут возникнуть не только за счет эксплуатационных ошибок или халатных действий, но и стать результатом преднамеренных противоправных действий отдельных сотрудников. Неправоверный доступ к конфиденциальным сведениям может быть также организован «извне», путем проведения разведывательных мероприятий, реализующих перехват информации по техническим каналам.

Техническая защита выделенных и защищаемых помещений проводится с целью обеспечения безопасности акустической информации ограниченного доступа, циркулирующей в данных помещениях.

Защита осуществляется с применением как пассивных, так и активных методов и технических средств, путем ослабления уровня информационных сигналов или снижения соотношения сигнал/шум в тракте передачи до величин, исключающих возможность перехвата за пределами контролируемой зоны.

Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, т. к. возможен ее перехват с помощью специальных технических средств контроля.

ГЛАВА 2. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АНАЛИЗА И ОБРАБОТКИ БОЛЬШИХ ОБЪЕМОВ ДАННЫХ

2.1. Обзор методов анализа больших объемов данных

С появлением сайтов социальных сетей и распространением цифровых вычислительных устройств и доступа в Интернет ежедневно генерируются огромные объемы общедоступных данных. Эффективные методы/алгоритмы для анализа этого огромного объема данных могут предоставлять практически в реальном времени информацию о возникающих тенденциях и обеспечивать раннее предупреждение чрезвычайных ситуаций. Кроме того, тщательный анализ этих данных может выявить множество полезных индикаторов социально-экономических и политических событий, которые могут помочь в разработке эффективной государственной политики. Основное внимание в данном разделе уделяется обзору применения аналитики больших данных в интересах развития общества в целом и повышения эффективности деятельности правоохранительных органов в частности. Появляющаяся способность использовать методы больших данных обещает значительно усовершенствовать различные сферы деятельности общества. Помимо всех преимуществ, крупномасштабное развертывание и внедрение систем обработки больших данных сталкивается с рядом проблем из-за огромного размера, быстро меняющегося и разнообразного характера данных. Наиболее насущные проблемы связаны с эффективным сбором и обменом данными, определением контекста (например, геолокации и времени) и достоверностью набора данных, а также обеспечением надлежащей конфиденциальности.

Избыток данных, поддерживаемый быстрым развитием технологий, увеличивается в геометрической прогрессии из-за растущей оцифровки всех аспектов современной жизни (с использованием таких технологий, как Интернет вещей (IoT), который использует датчики, например, в форме носимых устройств для предоставления данных, связанных с деятельностью человека и различными поведенческими моделями). Подсчитано, что мы генерируем 2,5 квинтиллиона байтов в день (отметим здесь, что квинтиллион байтов, или эксабайт, равен 10^{18} байтам) [3]. Был достигнут значительный прогресс в развитии возможностей обработки, хранения и анализа больших данных: в дополнение к вычислительным возможностям больших данных, быстрый прогресс в использовании интеллектуальных методов анализа данных, основанных на новых областях искусственного интеллекта (ИИ) и машинного обучения (МО), обеспечивает возможность обработки огромных объемов разнообразных неструктурированных данных, которые в настоящее время генерируются ежедневно, для извлечения ценных данных. действенные знания. Это дает

прекрасную возможность использовать эти данные для получения полезных знаний и идей.

С точки зрения больших данных серьезной проблемой является получение доступа к важным данным, связанным с людьми, которые часто находятся в исключительном доступе правительства в виде бумажных документов. К счастью, новая тенденция, известная как «открытые данные», которая способствует открытому публичному обмену данными от различных организаций государственного и частного секторов в доступных для поиска и машиночитаемых форматах, является благом для исследований БД. Правительства во всем мире все чаще внедряют проекты открытых данных для стимулирования инноваций и прозрачности. Кроме того, были разработаны платформы с открытым исходным кодом, которые облегчают создание и сбор цифровых данных с мобильных платформ. В то время как открытые данные можно по праву рассматривать как подмножество всех доступных больших данных: нюанс заключается в их ликвидности и достоверности. Открытые данные также способствуют культуре творчества и общественного благосостояния, о чем свидетельствуют различные турниры и конкурсы, организуемые для раскрытия потенциала открытых данных с точки зрения полезных мобильных приложений.

Современные наборы данных, или большие данные, отличаются от традиционных наборов данных тремя факторами: объемом, скоростью и разнообразием. В наше время огромные объемы данных генерируются с высокой скоростью, и многочисленные источники данных придают им огромное разнообразие. Все эти данные, при разумном использовании, могут по-настоящему реализовать понятие информационного века. Полезную информацию можно собрать из данных после выполнения интеллектуальной обработки и анализа доступных данных. В этом разделе рассматриваются методы (особенно связанные с машинным обучением) для сбора, хранения, обработки и анализа этого огромного объема данных.

Машинное обучение

Машинное обучение, подобласть искусственного интеллекта (ИИ), фокусируется на задаче, позволяющей вычислительным системам учиться на данных о том, как выполнять желаемую задачу автоматически. Машинное обучение имеет множество приложений, включая принятие решений, прогнозирование, и является ключевой технологией, позволяющей развертывать методы интеллектуального анализа данных и больших данных в различных областях здравоохранения, науки, техники, бизнеса и финансов. Вообще говоря, задачи МО можно разделить на следующие основные типы:

Обучение с учителем

В этом классе машинного обучения задача обучения состоит в том, чтобы обобщить обучающий набор, который помечен «руководителем» как содержащий информацию о классе примера, чтобы можно было делать прогнозы о новых, еще неизвестных событиях. Если результат (или прогноз) принадлежит непрерывному набору значений, то такая проблема называется регрессией, а если результат принимает дискретные значения, то проблема называется классификацией.

Методы обучения без учителя

Основным методом обучения без учителя является кластеризация. При кластеризации задача обучения состоит в том, чтобы классифицировать, не требуя маркированного обучающего набора, примеры на «кластеры» на основе воспринимаемого сходства. Эта кластеризация используется для поиска групп входных данных, которые имеют сходство по своим характеристикам. Интуитивно кластеризация похожа на классификацию без учителя: в то время как классификация в обучении с учителем предполагает наличие правильно помеченного обучающего набора, задача кластеризации без учителя направлена на непосредственное определение структуры входных данных.

Глубокое обучение

Глубокое обучение (ГО) – это метод машинного обучения, который включает в себя глубокие и сложные архитектуры [17, 18]. Эти архитектуры состоят из нескольких уровней обработки, каждый из которых способен генерировать нелинейный ответ, соответствующий входным данным. Эти уровни состоят из различных небольших процессоров, работающих параллельно для обработки предоставленных данных. Эти процессоры называются нейронами. ГО доказал свою эффективность в распознавании образов, обработке изображений и естественного языка [19]. ГО находит свое применение в очень широком спектре приложений, при этом многие ключевые технологические гиганты, такие как Google, IBM и Facebook, используют методы ГО для создания интеллектуальных продуктов.

Предсказательная аналитика

Предсказательная аналитика относится к технологии, которая направлена на обеспечение конкурентного преимущества путем прогнозирования некоторых будущих событий или поведения (с использованием методов интеллектуального анализа данных и машинного обучения) на основе прошлого опыта (в виде собранных данных). Прогнозная аналитика включает в себя науку о данных, машинное обучение, прогнозное и статистическое моделирование и выводит

эмпирические прогнозы на основе заданных входных эмпирических данных [26]. Основная предпосылка состоит в том, что будущее можно предсказать на основе прошлого опыта.

Интернет вещей

Интернет вещей (IoT) – это новое направление развития техники, подпитываемое ажиотажем вокруг больших данных, появлением науки о сетях [30], распространением устройств цифровой связи и повсеместным доступом к Интернету для простого населения. Технический отчет Глобального института McKinsey [2] представляет потенциал IoT с точки зрения экономической ценности. В IoT различные датчики и приводы подключаются через сеть к различным вычислительным системам, предоставляя данные для практических знаний. Таким образом, IoT, большие данные и сетевая наука связаны между собой. IoT находит свое применение в системах охранного мониторинга.

2.2. Современные инструменты анализа и обработки больших объемов данных

Мир больших данных с течением времени становится только больше. Организации всех отраслей из года в год производят все больше данных, и они находят все больше способов использовать эти данные для улучшения операций и повышения эффективности деятельности. Кроме того, руководители, стремящиеся быстрее извлечь пользу из данных, нуждаются в возможностях аналитики в реальном времени.

Все это требует значительных инвестиций в инструменты и технологии для работы с большими данными. За август 2021 года по некоторым экспертным оценкам ожидаемые мировые расходы на большие данные и системы аналитики составили 215,7 млрд долларов в 2021 году, что на 10,1% больше, чем в прошлом году. Также спрогнозировано, что расходы будут расти совокупным годовым темпом роста 12,8% до 2025 года.

Список технологий работы с большими данными огромен, и существует множество коммерческих продуктов, которые помогают организациям и учреждениям реализовать полный спектр инициатив в области аналитики на основе данных – от отчетов в реальном времени до приложений машинного обучения. Кроме того, существует множество инструментов для работы с большими данными с открытым исходным кодом, некоторые из которых также предлагаются в коммерческих версиях или в составе платформ для работы с большими данными и управляемых услуг.

Ниже представлен обзор наиболее популярных инструментов и технологий с открытым исходным кодом для управления и анализа больших данных, перечисленных в алфавитном порядке с кратким описанием их основных функций и возможностей.

1. Airflow

Airflow – это платформа управления рабочими процессами для планирования и запуска сложных конвейеров данных в системах больших данных. Это позволяет инженерам данных и другим пользователям гарантировать, что каждая задача в рабочем процессе выполняется в указанном порядке и имеет доступ к необходимым системным ресурсам. Airflow также рекламируется как простой в использовании: рабочие процессы создаются на языке программирования Python, и его можно использовать для построения моделей машинного обучения, передачи данных и различных других целей.

Airflow также включает следующие ключевые функции:

– модульная и масштабируемая архитектура, построенная на концепции направленных ациклических графов, которые иллюстрируют зависимости между различными задачами в рабочих процессах;

– пользовательский интерфейс веб-приложения для визуализации конвейеров данных, мониторинга их производственного статуса и устранения неполадок; а также готовые интеграции с основными облачными платформами и другими сторонними сервисами.

2. Delta Lake

Databricks Inc., поставщик программного обеспечения, основанный создателями механизма обработки Spark, разработал Delta Lake, а затем в 2019 году открыл исходный код технологии на основе Spark через Linux Foundation. Компания описывает Delta Lake как «уровень хранения открытого формата, который обеспечивает надежность, безопасность и производительность вашего озера данных как для потоковой передачи, так и для пакетных операций».

Delta Lake предназначен для создания единой базы структурированных, полуструктурированных и неструктурированных данных, устраняя хранилища данных, которые могут блокировать приложения для работы с большими данными. Кроме того, согласно данным Databricks, использование Delta Lake может помочь предотвратить повреждение данных, обеспечить более быстрые запросы, повысить актуальность данных и поддержать усилия по обеспечению соответствия.

3. Drill

Drill представляет собой распределенный механизм запросов с малой задержкой для крупномасштабных наборов данных, включая

структурированные и полуструктурированные/вложенные данные. Drill может масштабироваться на тысячи узлов кластера и способен запрашивать петабайты данных с помощью SQL и стандартных API-интерфейсов подключения.

Разработанный для изучения наборов больших данных, уровень детализации поверх нескольких источников данных позволяет пользователям запрашивать широкий спектр данных в различных форматах, от файлов последовательностей Hadoop и журналов сервера до баз данных NoSQL и облачных хранилищ объектов.

4. Druid

Druid – это аналитическая база данных в режиме реального времени, которая обеспечивает низкую задержку для запросов, высокий уровень параллелизма, многопользовательские возможности и мгновенную видимость потоковых данных. По словам его сторонников, несколько конечных пользователей могут одновременно запрашивать данные, хранящиеся в Druid, без ущерба для производительности.

Druid считается высокопроизводительной альтернативой традиционным хранилищам данных, которая лучше всего подходит для данных, управляемых событиями. Подобно хранилищу данных, он использует хранилище, ориентированное на столбцы, и может загружать файлы в пакетном режиме. Но он также включает в себя функции из поисковых систем и баз данных временных рядов, в том числе следующие:

– собственные инвертированные поисковые индексы для ускорения поиска и фильтрации данных;

– секционирование данных и запросы по времени;

– гибкие схемы со встроенной поддержкой полуструктурированных и вложенных данных.

5. Flink

Еще одна технология с открытым исходным кодом, Flink – это платформа обработки потоков для распределенных, высокопроизводительных и всегда доступных приложений. Он поддерживает вычисления с отслеживанием состояния как для ограниченных, так и для неограниченных потоков данных и может использоваться для пакетной, графической и итеративной обработки.

Одним из основных преимуществ, рекламируемых сторонниками Flink, является его скорость: он может обрабатывать миллионы событий в режиме реального времени с малой задержкой и высокой пропускной способностью. Flink, предназначенный для работы во всех распространенных кластерных средах, также включает следующие функции:

– вычисления в памяти с возможностью доступа к дисковому хранилищу при необходимости;

– три уровня API для создания различных типов приложений;

– набор библиотек для сложной обработки событий, машинного обучения и других распространенных вариантов использования больших данных.

6. Hadoop

Распределенная среда для хранения данных и запуска приложений на кластерах стандартного оборудования Hadoop была разработана как новаторская технология больших данных, помогающая обрабатывать растущие объемы структурированных, неструктурированных и частично структурированных данных. Впервые выпущенный в 2006 году, он на раннем этапе была почти синонимом больших данных; с тех пор ее частично затмили другие технологии, но она все еще широко используется.

Hadoop состоит из четырех основных компонентов:

– распределенная файловая система Hadoop (HDFS), которая разбивает данные на блоки для хранения на узлах в кластере, использует методы репликации для предотвращения потери данных и управляет доступом к данным;

– YARN, сокращение от Yet Another Resource Negotiator, которое планирует выполнение заданий на узлах кластера и выделяет им системные ресурсы;

– Hadoop MapReduce, встроенный механизм пакетной обработки, который разделяет большие вычисления и запускает их на разных узлах для ускорения и балансировки нагрузки; а также

– Hadoop Common, общий набор утилит и библиотек.

7. Hive

Hive – это программное обеспечение инфраструктуры хранилища данных на основе SQL для чтения, записи и управления большими наборами данных в распределенных средах хранения. Hive работает поверх Hadoop и используется для обработки структурированных данных. Используется для суммирования и анализа данных, а также для запросов к большим объемам данных. Хотя его нельзя использовать для онлайн-обработки транзакций, обновлений в реальном времени, а также запросов или заданий, требующих извлечения данных с малой задержкой, разработчики описывают Hive как масштабируемый, быстрый и гибкий.

Другие ключевые особенности включают следующее:

– стандартные функции SQL для запросов и анализа данных;

– встроенный механизм, помогающий пользователям структурировать различные форматы данных;

– доступ к файлам HDFS и файлам, хранящимся в других системах, таких как база данных Apache HBase.

8. HPCC Systems

HPCC Systems – это платформа для обработки больших данных, разработанная LexisNexis. В полном соответствии со своим полным названием – высокопроизводительный вычислительный кластер – эта технология по своей сути представляет собой кластер компьютеров, построенных из стандартного оборудования для обработки данных.

Готовая к работе платформа, обеспечивающая быструю разработку и исследование данных, HPCC Systems включает три основных компонента:

1) Thor – механизм обработки данных, который используется для очистки, объединения и преобразования данных, а также для их профилирования, анализа и подготовки к использованию в запросах;

2) Roxie, механизм доставки данных, используемый для доставки подготовленных данных с нефтеперерабатывающего завода;

3) Enterprise Control Language (ECL), язык программирования для разработки приложений.

9. Hudi

Hudi – это сокращение от Hadoop Upserts Deletes and Incrementals. Еще одна технология с открытым исходным кодом, используется для управления приемом и хранением больших наборов аналитических данных в файловых системах, совместимых с Hadoop.

Hudi, впервые разработанный Uber, предназначен для обеспечения эффективного приема и подготовки данных с малой задержкой. Кроме того, он включает в себя структуру управления данными, которую организации могут использовать для выполнения следующих задач:

– упростить добавочную обработку данных и разработку конвейера данных;

– улучшить качество данных в системах больших данных;

– управлять жизненным циклом наборов данных.

10. Iceberg

Iceberg – это формат открытых таблиц, используемый для управления данными в хранилищах, что частично достигается за счет отслеживания отдельных файлов данных в таблицах, а не за счет отслеживания каталогов. Как заявляет разработкчик: «Iceberg обычно используется в производстве, где одна таблица может содержать десятки петабайт данных».

Разработанный для улучшения стандартных макетов, существующих в таких инструментах, как Hive, Presto, Spark и Trino, формат таблиц Iceberg имеет функции, аналогичные таблицам SQL в реляционных базах данных. Однако он также поддерживает несколько механизмов, работающих с одним и тем же набором данных. Другие примечательные особенности включают следующее:

– эволюция схемы для изменения таблиц без необходимости перезаписи или переноса данных;

– скрытое разделение данных, которое избавляет пользователей от необходимости поддерживать разделы;

– возможность «путешествия во времени», поддерживающая воспроизводимые запросы с использованием одного и того же моментального снимка таблицы.

11. Kafka

Kafka – это распределенная платформа потоковой передачи событий, которая, по данным Apache, используется более чем 80% компаний из списка Fortune 100 и тысячами других организаций для высокопроизводительных конвейеров данных, потоковой аналитики, интеграции данных и критически важных приложений. Проще говоря, Kafka – это фреймворк для хранения, чтения и анализа потоковых данных.

Эта технология разделяет потоки данных и системы, сохраняя потоки данных, чтобы их можно было использовать в другом месте. Он работает в распределенной среде и использует высокопроизводительный сетевой протокол TCP для связи с системами и приложениями.

Ниже приведены некоторые из ключевых компонентов Kafka:

– набор из пяти основных API для Java и языка программирования Scala;

– отказоустойчивость как серверов, так и клиентов в кластерах Kafka;

– эластичная масштабируемость до 1000 серверов хранения на кластер.

12. Kylin

Kylin – это распределенное хранилище данных и аналитическая платформа для больших данных. Он предоставляет механизм оперативной аналитической обработки или OLAP, предназначенный для поддержки очень больших наборов данных. Поскольку Kylin построен на основе таких технологий как Hadoop, Hive, Parquet и Spark. Его можно легко масштабировать для обработки больших объемов данных.

Скорость отправки запроса и получения ответа измеряется в миллисекундах. Кроме того, Kylin предоставляет простой интерфейс для многомерного анализа больших данных и интегрируется с другими

инструментами анализа процессов предприятий. Первоначально Kylin был разработан eBay, который в 2014 году представил его как технологию с открытым исходным кодом.

13. Presto

Этот механизм запросов SQL с открытым исходным кодом, ранее известный как PrestoDB, может одновременно обрабатывать как быстрые запросы, так и большие объемы данных в распределенных наборах данных. Presto оптимизирован для интерактивных запросов с малой задержкой и масштабируется для поддержки аналитических приложений с несколькими петабайтами данных в хранилищах данных и других репозиториях.

Разработка Presto началась в 2012 году. В 2018 году технология разделилась на две ветви: PrestoDB и PrestoSQL. Так продолжалось до декабря 2020 года, когда PrestoSQL был переименован в Trino, а PrestoDB вернулась к имени Presto. Проект с открытым исходным кодом Presto в настоящее время находится под контролем Presto Foundation, созданной как часть Linux Foundation в 2019 году.

14. Samza

Samza – это распределенная система потоковой обработки, созданная LinkedIn и теперь являющаяся проектом с открытым исходным кодом. Samza позволяет пользователям создавать приложения с отслеживанием состояния, которые могут обрабатывать данные в режиме реального времени из Kafka, HDFS и других источников.

Система может работать поверх Hadoop или Kubernetes, а также предлагает вариант автономного развертывания. Samza может обрабатывать «несколько терабайт» данных о состоянии с малой задержкой и высокой пропускной способностью для быстрого анализа данных. Благодаря унифицированному API он также может использовать тот же код, написанный для заданий потоковой передачи данных, для запуска пакетных приложений. Другие функции включают следующее:

– встроенная интеграция с Hadoop, Kafka и рядом других платформ данных;

– возможность работать с встроенной библиотекой в приложениях Java и Scala;

– имеются отказоустойчивые функции, предназначенные для обеспечения быстрого восстановления после системных сбоев.

15. Spark

Spark – это механизм обработки и анализа данных в памяти, который может работать в кластерах, управляемых Hadoop, Mesos и Kubernetes, или в автономном режиме. Он обеспечивает крупномасштабное

преобразование и анализ данных и может использоваться как для пакетных, так и для потоковых приложений, а также для машинного обучения и обработки графов.

Доступ к данным можно получить из различных источников, включая HDFS, реляционные базы данных и базы данных NoSQL. Spark также поддерживает различные форматы файлов и предлагает разнообразный набор API для разработчиков.

Главное преимущество данного инструмента – это скорость: разработчики Spark утверждают, что он может работать до 100 раз быстрее, чем традиционный аналог MapReduce, при выполнении пакетных заданий при обработке в памяти. В результате Spark стал лучшим выбором для многих пакетных приложений в средах больших данных, а также функционировал как механизм общего назначения.

16. Storm

Еще одна технология с открытым исходным кодом, Storm – это распределенная система вычислений в реальном времени, предназначенная для надежной обработки неограниченных потоков данных. Согласно информации о проекте, его можно использовать для приложений, которые включают аналитику в реальном времени, онлайн-машинное обучение и непрерывные вычисления, а также задания на извлечение, преобразование и загрузку.

Кластеры Storm похожи на кластеры Hadoop, но приложения продолжают работать на постоянной основе, если их не остановить. Система отказоустойчива и гарантирует обработку данных. Storm можно использовать с любым языком программирования, системой очередей сообщений и базой данных. Также включает в себя следующие элементы:

– функция Storm SQL, позволяющая выполнять запросы SQL к наборам потоковых данных;

– Trident и Streams API, два других высокоуровневых интерфейса для обработки в Storm;

– использование технологии Apache Zookeeper для координации кластеров.

17. Trino

Trino – это одна из двух ветвей механизма запросов Presto.Trino позволяет пользователям запрашивать данные независимо от того, где они хранятся, с поддержкой собственных запросов в Hadoop и других хранилищах данных. Также следует учитывать: базы данных NoSQL

Базы данных NoSQL – еще один важный тип технологии больших данных. Они нарушают традиционную структуру реляционных баз данных на основе SQL, поддерживая гибкие схемы, что делает их хорошо подходящими для обработки огромных объемов всех типов данных,

особенно неструктурированных и полуструктурированных, которые не подходят для строгих схем, используемых в реляционных базах данных.

Программное обеспечение NoSQL появилось в конце 2000-х, чтобы помочь справиться с растущими объемами разнообразных данных, которые организации генерировали, собирали и анализировали в рамках инициатив по работе с большими данными. С тех пор базы данных NoSQL получили широкое распространение и теперь используются в организациях различных отраслей.

Кроме того, сами базы данных NoSQL бывают разных типов, которые поддерживают разные приложения для работы с большими данными. Это четыре основные категории NoSQL с примерами доступных технологий в каждой из них:

1. Базы документов. Они хранят элементы данных в структурах, подобных документам, используя такие форматы, как JSON. Примеры включают Apache CouchDB, Couchbase Server, MarkLogic и MongoDB.

2. Графические базы данных. Они соединяют «узлы» данных в графоподобных структурах, чтобы подчеркнуть отношения между элементами данных. Примеры включают AllegroGraph, Amazon Neptune и Neo4j.

3. Хранилища ключ-значение. Они объединяют уникальные ключи и связанные значения в относительно простую модель данных, которую можно легко масштабировать. Примеры включают Aerospike, Amazon DynamoDB и Redis.

4. Базы данных с широкими столбцами. Они хранят данные в таблицах, которые могут содержать очень большое количество столбцов для обработки большого количества элементов данных. Примеры включают Cassandra, Google Cloud Bigtable и HBase.

2.3. Основные тенденции развития технологий анализа и обработки больших объемов данных

Работа с большими данными – это больше, чем просто работа с большими объемами хранимой информации. Объем – это лишь один из многих критериев больших данных, которые организациям необходимо решить. Обычно также существует значительное разнообразие данных – от структурированной информации, хранящейся в базах данных, распределенных по всей организации, до огромного количества неструктурированных и полуструктурированных данных, находящихся в файлах, изображениях, видео, датчиках, системных журналах, тексте и документах, в том числе бумажных. ждут оцифровки. Кроме того, эта информация часто создается и изменяется с большой скоростью (скоростью) и имеет разный уровень качества данных (достоверность), что

создает дополнительные проблемы при управлении данными, их обработке и анализе.

Существуют четыре основные тенденции развития в области анализа и обработки больших данных.

1. Больше данных, увеличение разнообразия данных способствуют прогрессу в обработке и развитию периферийных вычислений.

Неудивительно, что скорость генерации данных продолжает увеличиваться. Большая часть этих данных генерируется не из транзакций, происходящих в базах данных, а из других источников, включая облачные системы, интеллектуальные устройства, такие как смартфоны и голосовые помощники, а также потоковое видео. Эти данные в значительной степени неструктурированы и в прошлом в основном оставались необработанными и неиспользованными организациями, превращая их в так называемые темные данные.

Это подводит нас к самой большой тенденции в области больших данных: источники, не являющиеся базами данных, будут по-прежнему оставаться доминирующими генераторами данных, что, в свою очередь, заставит организации пересмотреть свои потребности в обработке данных. Голосовые помощники и устройства IoT, в частности, способствуют быстрому росту потребностей в управлении большими данными в разных отраслях, в том числе и в правоохранительном сегменте. Этот взрыв разнообразия данных заставляет организации думать не только о традиционных хранилищах данных, но и о средствах обработки всей этой информации.

Кроме того, необходимость обработки генерируемых данных перемещается на сами устройства, поскольку отраслевые прорывы в вычислительной мощности привели к разработке все более совершенных устройств, способных самостоятельно собирать и хранить данные, не нагружая сеть, хранилище и вычислительную инфраструктуру. Например, мобильные банковские приложения могут выполнять множество задач по удаленному внесению и обработке чеков без необходимости отправлять изображения туда и обратно в центральные банковские дата-центры для обработки.

В знак того, что все это выходит на первый план, исследование планов расходов на ИТ на 2022 год, проведенное подразделением Enterprise Strategy Group TechTarget, показало, что главными приоритетами организаций для поддержки своих инициатив в области данных являются продвижение использования технологий следующего поколения, перемещение переносить данные из устаревших систем в современные и расширять возможности обработки данных там, где они были созданы.

Использование устройств для распределенной обработки воплощено в концепции граничных вычислений, которая перекладывает

вычислительную нагрузку на сами устройства до отправки данных на серверы. Пограничные вычисления оптимизируют производительность и хранилище, уменьшая потребность в передаче данных по сетям, снижая затраты на вычисления и обработку, особенно на облачное хранилище, пропускную способность и затраты на обработку. Пограничные вычисления помогают ускорить анализ данных и быстрее реагируют на запросы пользователя.

Например, в секторе здравоохранения быстро растущий рынок носимых устройств, таких как Fitbit, Apple Watch и устройства Google Android, стимулирует рост телемедицины и позволяет поставщикам медицинских услуг собирать важные данные о пациентах в режиме реального времени. Результаты используются для широкого спектра приложений для обработки больших данных и аналитики, предназначенных для улучшения результатов лечения пациентов.

Большие данные вызывают серьезные изменения в том, как организации обрабатывают, хранят и анализируют данные.

2. Потребность в хранении больших данных стимулирует инновации в облачных и гибридных облачных платформах, рост хранилищ данных.

Чтобы справиться с неумолимым увеличением объема генерируемых данных, организации тратят больше своих ресурсов на хранение этих данных в ряде облачных и гибридных облачных систем, оптимизированных для всех категорий больших данных. В предыдущие десятилетия организации управляли собственной инфраструктурой хранения, что приводило к созданию огромных центров обработки данных, которыми предприятия должны были управлять, защищать и эксплуатировать. Переход к облачным вычислениям изменил эту динамику. Перекладывая ответственность на поставщиков облачной инфраструктуры организации могут работать с почти неограниченными объемами новых данных и платить за хранение и вычислительные мощности по требованию без необходимости поддерживать свои собственные большие и сложные дата-центры.

Некоторые отрасли сталкиваются с трудностями при использовании облачной инфраструктуры из-за нормативных или технических ограничений. Например, строго регулируемые отрасли, такие как здравоохранение, финансовые услуги и правительство, имеют ограничения, препятствующие использованию общедоступной облачной инфраструктуры. Таким образом, за последнее десятилетие поставщики облачных услуг разработали способы предоставления более удобной для регулирования инфраструктуры, а также гибридные подходы, которые сочетают аспекты сторонних облачных систем с локальными вычислениями и хранилищем для удовлетворения критических потребностей инфраструктуры. Эволюция как общедоступных, так и

гибридных облачных инфраструктур, несомненно, будет продолжаться по мере того, как организации ищут экономические и технические преимущества облачных вычислений.

Помимо инноваций в области облачного хранения и обработки, предприятия переходят на новые подходы к архитектуре данных, которые позволяют им справляться с проблемами разнообразия, достоверности и объема больших данных. Вместо того, чтобы пытаться централизовать хранение данных в хранилище данных, которое требует сложного и трудоемкого извлечения, преобразования и загрузки данных, предприятия развивают концепцию так называемы озер данных. Озера данных хранят структурированные и неструктурированные наборы данных в их собственном формате. Этот подход переносит ответственность за преобразование и обработку на конечные точки, которые имеют разные потребности в данных. Озеро данных также может предоставлять общие сервисы для анализа и обработки данных.

3. Внедрение расширенной аналитики, машинного обучения и других технологий искусственного интеллекта резко возрастает.

При огромном количестве генерируемых данных традиционные подходы к аналитике сталкиваются с трудностями, поскольку их нелегко автоматизировать для масштабного анализа данных. Технологии распределенной обработки, особенно продвигаемые платформами с открытым исходным кодом, такими как Hadoop и Spark, позволяют организациям обрабатывать петабайты информации с высокой скоростью. Системы машинного обучения и искусственного интеллекта позволяют им легче выявлять закономерности, выявлять аномалии и делать прогнозы, чем раньше. Предприятия используют технологии аналитики больших данных для оптимизации своих инициатив в области бизнес-аналитики и аналитики, переходя от медленных инструментов отчетности, зависящих от технологии хранилища данных, к более интеллектуальным, быстро реагирующим приложениям, которые обеспечивают большую прозрачность поведения клиентов, бизнес-процессов и операций в целом.

Ни одна технология не была столь революционной для аналитики больших данных, как системы машинного обучения и искусственного интеллекта. ИИ используется организациями любого размера для оптимизации и улучшения своих бизнес-процессов. Машинное обучение позволяет им легче выявлять шаблоны и обнаруживать аномалии в больших наборах данных, чтобы обеспечить прогнозную аналитику и другие расширенные возможности анализа данных. Сюда входят системы распознавания изображений, видео и текстовых данных; автоматизированная классификация информации; возможности обработки естественного языка для чат-ботов и анализа голоса и текста; автономная

автоматизация бизнес-процессов; высокая степень персонализации и рекомендации; и системы, которые могут найти оптимальные решения.

Действительно, с помощью искусственного интеллекта и машинного обучения компании используют свои среды больших данных для обеспечения более глубокой поддержки клиентов с помощью интеллектуальных чат-ботов и более персонализированного взаимодействия, не требуя значительного увеличения штата службы поддержки клиентов. Подобные технологии могут найти применение в правоохранительном сегменте при взаимодействии с гражданами. Эти системы с поддержкой ИИ способны собирать и анализировать огромные объемы информации о клиентах и пользователях, особенно в сочетании со стратегией озера данных, которая может собирать широкий спектр информации из многих источников.

Предприятия также видят инновации в области визуализации данных. Люди понимают значение данных, когда они представлены в наглядной форме, такой как диаграммы, графики и графики. Появляющиеся формы визуализации данных предоставляют возможности аналитики с поддержкой ИИ даже обычным бизнес-пользователям. Это помогает организациям выявлять ключевые идеи, которые могут улучшить процесс принятия решений. Компании открывают для себя ценность принятия решений на основе данных и силу данных во всей организации. Расширенные формы инструментов визуализации и аналитики позволяют пользователям даже задавать вопросы на естественном языке, при этом система автоматически определяет правильный запрос и отображает результаты в зависимости от контекста.

4. DataOps и управление данными выходят на первый план.

Многие аспекты обработки, хранения и управления большими данными будут развиваться еще долгие годы. Большая часть этих инноваций обусловлена технологическими потребностями, а также частично изменениями в том, как мы думаем о данных и относимся к ним.

Одной из областей инноваций является появление DataOps, методологии и практики, которые фокусируются на гибких, итерационных подходах к работе с полным жизненным циклом данных, когда они проходят через организацию. Вместо того, чтобы думать о данных по частям с отдельными людьми, занимающимися созданием, хранением, транспортировкой, обработкой и управлением данными, процессы и платформы DataOps удовлетворяют организационные потребности на протяжении всего жизненного цикла данных от создания до архивирования.

Точно так же организации все чаще сталкиваются с вопросами управления данными, конфиденциальности и безопасности. В прошлом предприятия часто не слишком заботились о конфиденциальности данных

и управлении ими, но новые правила делают их гораздо более ответственными за то, что происходит с личной информацией в их системах. Появляются новые инструменты, чтобы гарантировать, что данные остаются там, где они должны оставаться, защищены в состоянии покоя и в движении и надлежащим образом отслеживаются на протяжении всего их жизненного цикла.

В совокупности эти тенденции в области больших данных делают работу в пространстве больших данных интересной в 2022 году и, без сомнения, в обозримом будущем.

ГЛАВА 3. ИНТЕГРАЦИЯ АЛГОРИТМОВ ВИДЕОАНАТИЛИКИ В СИСТЕМАХ ОХРАННОГО ТЕЛЕВИДЕНИЯ

3.1. Задачи систем охранного телевидения

В последнее время одним из самых перспективных направлений развития систем безопасности считается использование на объектах систем охранного телевидения (СОТ). На настоящий момент неоспорима целесообразность применения таких систем для усиления охраны объектов.

Телевизионное изображение способно передавать уникальную информацию о ситуации на охраняемом объекте либо о поведении и индивидуальных особенностях нарушителя, что делает в ряде случаев СОТ незаменимыми для обеспечения безопасности объекта.

Специфика систем охранного телевидения заключается в широком спектре функций, которые они способны выполнять, в зависимости от выбранной конфигурации. Например, в торговых залах, демонстративно установленные камеры видеонаблюдения способны оказать психологическое давление на потенциальных преступников. СОТ так же способны брать на себя некоторые функции систем охранной и пожарной сигнализации. Современные технологии интеллектуального видео позволяют использовать системы охранного телевидения для идентификации лиц, автомобильного и железнодорожного транспорта.

Использование СОТ особенно актуально на объектах, обладающих протяженным периметром, где в некоторых случаях телевизионные системы использовать экономически выгоднее и значительно более информативно, чем периметральные системы охраны.

Системы охранного телевидения являются неотъемлемой частью интегрированных систем безопасности. Они достаточно легко интегрируются на любых уровнях с системами охранной и пожарной сигнализации, а также с системами контроля и управления доступом.

Рассматривая возможности применения в охранной сигнализации телевизионных систем (систем охранного телевидения – СОТ по терминологии ГОСТ Р 51558-2014) можно определить круг их задач, исходя из требований обеспечения безопасности и учета всей структуры охраны объекта:

- оперативные задачи по охране;
- наблюдение за охраняемым объектом;
- видеозапись (видеорегистрация).

При реализации первых двух из вышеназванных задач, стоящих перед СОТ, в настоящее время возникает определенный набор проблем, затрудняющих эффективное использование таких систем.

Использование детекции движения в современных СОТ позволяет автоматизировать в некоторой степени наблюдение за зонами видеоконтроля, что дает возможность обслуживания одним оператором большого количества камер, однако это возможно лишь в случае наблюдения за зонами, в которых движение в период охраны практически отсутствует (зоны отчуждения, внутренняя территория объекта в ночное время и пр.), что не дает возможности использовать функциональный потенциал СОТ в полной мере. С другой стороны, наиболее эффективно использование телевизионных систем для наблюдения за зонами, в которых движение осуществляется постоянно (торговые залы, музеи, казино и пр.) однако в этих условиях применение детекторов движения нецелесообразно, что резко сокращает количество видеокамер, обслуживаемых одним оператором.

Среди задач, решаемых СОТ, можно отметить особое значение видеорегистрации. Хотя она непосредственно и не решает вопросы охраны, но ей принадлежит существенная роль в раскрытии преступлений и противоправных действий, а широкое внедрение телевизионных систем с мощными средствами видеорегистрации может способствовать профилактике и предупреждению противоправных действий.

В настоящее время системы охранного телевидения развиваются по нескольким направлениям, считающимся одними из самых перспективных направлений развития систем безопасности в целом. Тенденции снижения цен на аппаратуру видеонаблюдения, активное внедрение цифровых систем, развитие каналов передачи информации позволяют использовать СОТ во всех сферах безопасности различных уровней сложности, от видеоглазков до построения систем безопасности таких объектов как банки, аэропорты, систем «Безопасный город».

3.2. Классификация и принципы построения систем охранного телевидения

Основными аппаратными компонентами современных систем охранного телевидения являются видеокамеры и платы видеоввода видеосигнала в видеорегистратор (видеосервер), который и берет на себя все функции обработки и записи видеоизображений (рис. 1), заменяя собой мультиплексоры, квадраторы, видеомагнитофоны и коммутаторы, использовавшиеся для построения СОТ ранее. Основная роль в обработке видеосигнала отводится программному обеспечению.

К дополнительным аппаратным компонентам систем охранного телевидения можно отнести устройства видеопамяти, управления камерами, устройства инфракрасной подсветки, поворотные устройства и пр.

СОТ могут быть классифицированы по двум основным критериям: в зависимости от решаемых ими целевых задач видеоконтроля и по виду наблюдения (рис. 1, 2).

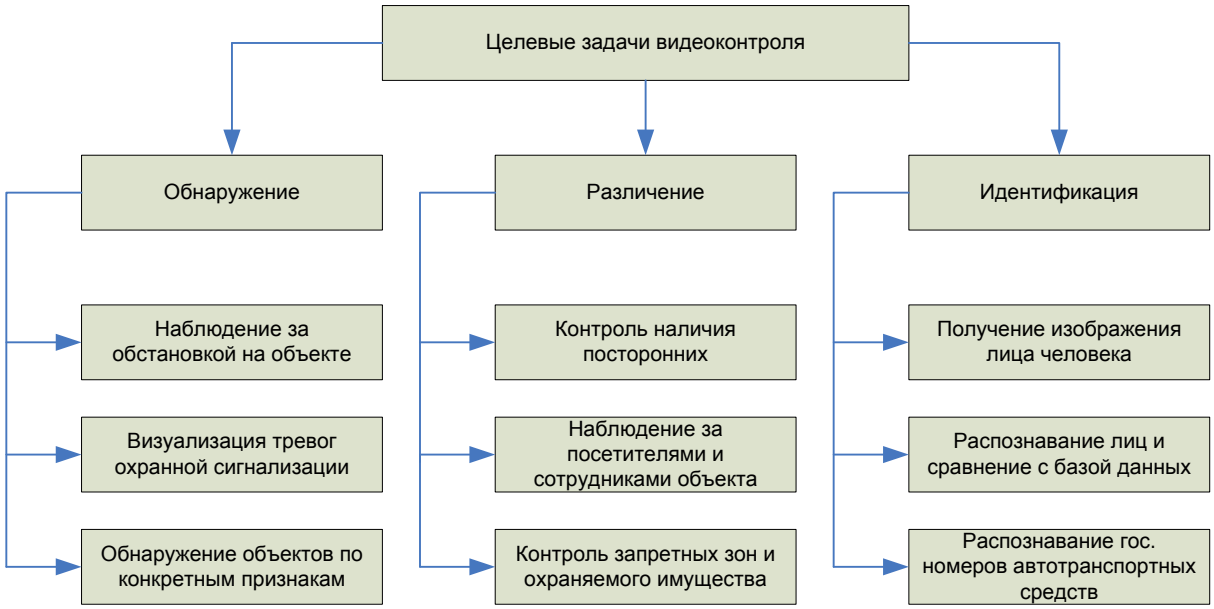

Рис. 1. Классификация СОТ в зависимости от решаемых ими целевых задач видеоконтроля

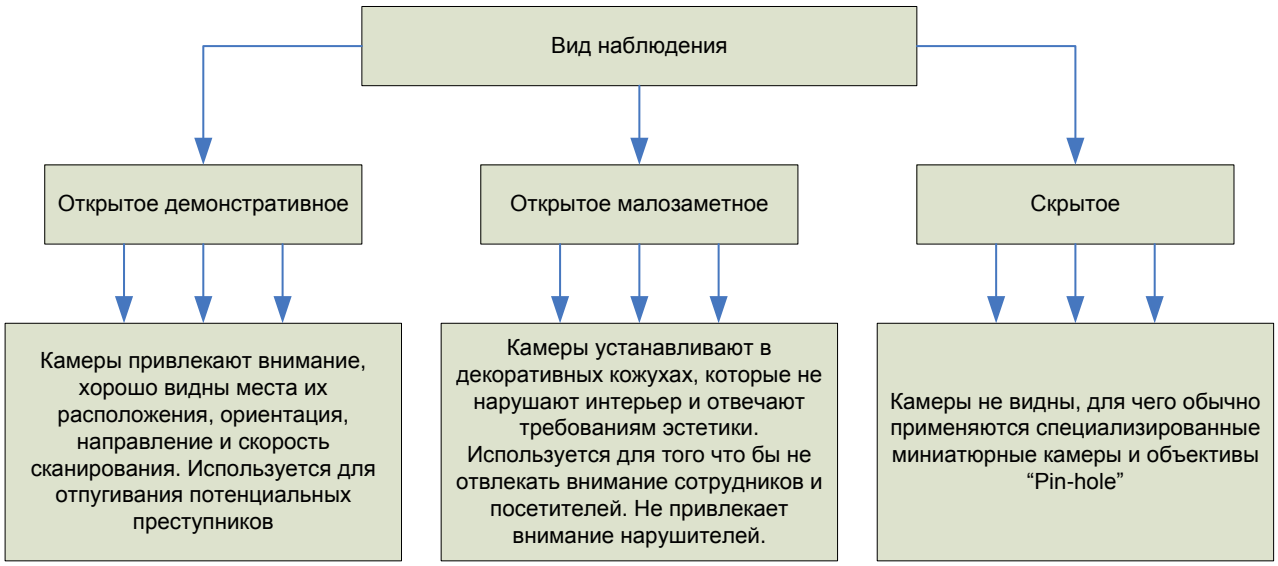

Рис. 2. Классификация СОТ в зависимости от вида наблюдения

3.3. Типовые варианты построения систем охранного телевидения

В зависимости от величины расстояния, на которые нужно увеличить прохождение сигнала можно использовать вставки на оптоволоконном кабеле или на коаксиальном экранированном кабеле (рис. 3-7).

Варианты использования оптоволоконных вставок

Рис. 3. Схема удаленного (до 2 км) подключения 4-х IP камер к сетевому видеорегистратору по оптоволоконному кабелю.

Рис. 4. Схема удаленного (до 2 км) подключения одной IP камеры к сетевому видеорегистратору по оптоволоконному кабелю.

Варианты использования вставок на коаксиальном кабеле

Рис. 5. Схема удаленного (до 1,2 км) подключения 4-х IP камер к сетевому видеорегистратору по коаксиальному кабелю

Рис. 6. Схема удаленного подключения (до 1,8 км) одной IP видеокамеры к сетевому видеорегистратору по коаксиальному кабелю

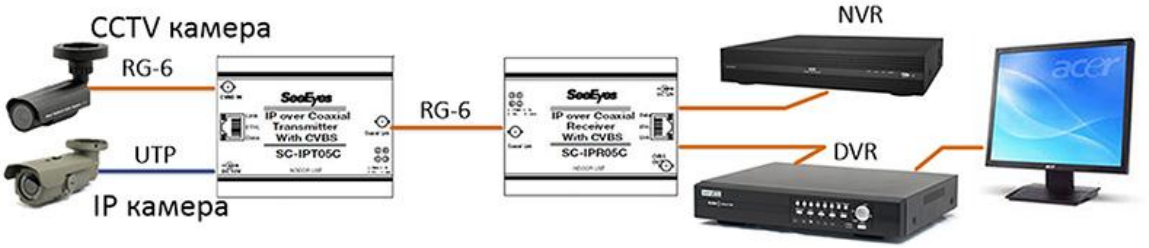

Рис. 7. Передача по коаксиалу сигнала от CCTV и IP камер до 600м

3.4. Видеоаналитика. Понятие, задачи, классификация и принцип работы

Системы охранного телевидения являются разновидностью прикладных телевизионных систем, предназначенных для решения специфических задач, меньших по масштабу, чем задачи вещательного телевидения. Данные системы функционируют на основе общих с вещательными системами физических принципах, однако сфера их применения определяет структуру их построения, параметры и

выполняемые функции в зависимости от специфики решаемых задач и условий применения.

Основное назначение СОТ, как и системы вещательного телевидения, заключается в передаче на расстояние изображения объекта. В случае с вещательным телевидением изображение просто воспринимается зрителем без оказания воздействия в отношении объекта. Охранная функция СОТ обусловлена необходимостью защиты объекта от преступных посягательств. Анализируя изображение охраняемого объекта возможно прогнозировать развитие ситуации, предупреждать противоправные деяния или своевременно на них реагировать за счет получения информации в режиме реального времени.

В случае наблюдения за обширной территорией или за большим количеством объектов идеальным вариантом было бы использование одной видеокамеры и устройства отображения (видеомонитора). Однако в силу принципа работы видеокамеры размеры зоны видеоконтроля ограничены даже у камер с широкоугольным объективом. Поэтому расширение области наблюдения неизбежно приводит к увеличению количества видеокамер в системе. Наряду с этим увеличение количества изображений на экране видеомонитора приводит к уменьшению их размера, что затрудняет их восприятие и анализ, а в некоторых случаях делает невозможным выполнение оператором своих функций. Разумным решением в этом случае является увеличение размеров устройств воспроизведения или их количества. Однако здесь тоже есть пределы, обусловленные физиологией зрительного аппарата человека, в частности размерами полей зрения по вертикали и горизонтали. Кроме того, немаловажным является время непрерывного и эффективного анализа изображения. По мере его увеличения зрительный аппарат утомляется, внимание притупляется, в результате чего реакция на события может увеличиваться, а некоторые из них могут и вовсе остаться незамеченными.

Стремление осуществлять наблюдение на большей территории и за большим количеством объектов с целью предупреждения и оперативного реагирования на различные инциденты не только в местах их наиболее вероятного возникновения приводит к увеличению количества видеокамер и устройств воспроизведения. Это в свою очередь приводит к закономерному увеличению штата операторов и повышению затрат и сложности организации их работы. В этом случае наиболее эффективным и рациональным представляется использование технических и программных средств, выполняющих некоторые функции оператора, например, предварительный анализ изображений и выделение полезной информации. Такая возможность появилась благодаря развитию информационно-телекоммуникационных технологий, средств вычислительной техники и программного обеспечения.

Важным моментом при эксплуатации СОТ является организация хранения видеоинформации. Для выполнения СОТ функции видеорегистрации требуется наличие хранилища, позволяющего хранить видеоархив различного размера. По мере увеличения количества видеокамер и повышения разрешения изображений размер хранилища увеличивается. Размер хранилища непосредственно влияет на размер архива. В разных сферах применения СОТ требования к глубине (продолжительности интервала времени записи) архива, устанавливаемые нормативными документами, отличаются, однако на практике глубина архива составляет 30 суток и более. Это обусловлено практикой выявления, расследования и раскрытия преступлений и административных правонарушений. Обычно этого времени достаточно для проведения всех необходимых мероприятий.

Терминологический аппарат в любой предметной области появляется не сразу, а формируется по мере ее развития по аналогии с внесением поправок в законодательные акты, что может быть обусловлено появлением новых обстоятельств, развитием науки и техники и т.д.

Телевидение как наука развивается уже более 100 лет, начав свой путь с этапа зарождения идей. Системы охранного телевидения как отдельный вид прикладных телевизионных систем существуют несколько десятков лет. За этот период ведущими экспертами, разработчиками и производителями оборудования сформирован емкий перечень терминов и определений, однако по мере развития этих систем появляются новые понятия. Так было с функцией системы, заключающейся в автоматическом анализе изображений и выявлении различных событий в кадре. До определенного времени не существовало понятия, связанного с данной функцией.

Основными нормативными документами, содержащими термины и определения в области систем охранного телевидения, являются ГОСТ Р 52551-2016 Системы охраны и безопасности. Термины и определения и ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний, причем первый из них ссылается в части определений на второй, что и логично, так как он был утвержден ранее. В предыдущей версии стандарта по СОТ от 2008 года содержался относительно короткий перечень терминов. В новой версии данный перечень был расширен почти в два раза. Появилось новое понятие «видеоаналитика».

Термин «видеоаналитика» состоит из двух частей: «видео» (от лат. vidēre «видеть») и «аналитика» (от др.-греч. ἀναλυτικά «буквально: искусство анализа», далее от др.-греч. ἀνάλυσις «разложение, растворение»). Таким образом данный термин исходя из происхождения его частей дословно можно перевести как анализ визуальной информации, то есть информации, которая может восприниматься зрительным

аппаратом человека. Данный термин появился в области СОТ до его закрепления в стандарте и на тот момент не существовало однозначного определения. Некоторые эксперты понимали под ним процесс автоматического анализа изображений, другие отождествляли его как программное обеспечение, осуществляющее данную функцию СОТ. Согласно последней редакции основного ГОСТ в области СОТ видеоаналитикой (video analytics) называют программное обеспечение, реализующее алгоритмы автоматизированного получения различных данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей. Таким образом данная функция может осуществляться в режиме реального времени (онлайн) и постфактум (офлайн), причем во втором случае процесс может повторятся многократно.

Наряду с понятием «видеоаналитика» существует такой термин как «компьютерное зрение» (машинное зрение). Эти понятия относятся к одной области знаний, однако не являются равнозначными. Видеоаналитика является составной частью компьютерного зрения в части анализа изображения. Компьютерное зрение (computer vision) – это технология получения и обработки визуальной информации с помощью ЭВМ. Компьютерное зрение применяется там, где в силу возможностей зрительного аппарата человеку затруднительно выполнение каких-либо операций, либо опасно или вообще невозможно.

Использование информационно-телекоммуникационных технологий, ЭВМ и программного обеспечения позволяет применять видеоаналитику в различных областях человеческой деятельности, таких как промышленность, медицина, наука, образование, финансовый сектор, торговля. Наибольший интерес для правоохранительных органов представляет использование видеоаналитики при обеспечении безопасности объектов и территорий, охраны общественного порядка и обеспечения общественной безопасности, поиска розыскиваемых лиц, предупреждения, расследования и раскрытия преступлений и административных правонарушений.

Видеоаналитика позволяет обнаруживать, распознавать и идентифицировать различные объекты (люди, животные, транспорт, предметы), явления (огонь, дым), анализировать поведение объектов (появление, перемещение, исчезновение), осуществлять автоматизированный поиск необходимой видеоинформации в архиве по заданным критериям и многое другое.

Видеоаналитика может применятся к прошедшим, текущим и будущим явлениям. Если событие уже произошло, то ведется работа с архивом, осуществляется поиск и обнаружение необходимых фрагментов. Ранее этот процесс был очень трудоемок и занимал много времени. Если приблизительные дата и время события были заранее неизвестны, то

приходилось вручную просматривать весь архив, а в некоторых случаях по несколько раз, так как продолжительность некоторых событий пренебрежимо мала по сравнению с продолжительностью архива и необходимые фрагменты могли быть просто пропущены при ускоренном просмотре.

В режиме реального времени видеоаналитика может использоваться для обнаружения событий, предшествующих опасным явлениям, например, обнаружение оставленных подозрительных предметов (коробок, ящиков, сумок и т.п.), замаскированных под взрывное устройство. В этом случае оператору выдается предупреждение (текстовое сообщение, звуковой сигнал, выделение цветом области экрана и т.д.), позволяющее оценить ситуацию и предпринять меры до наступления опасного явления.

Возможности видеоаналитики позволяют с определенной вероятностью предсказывать события на основе информации о прошедших и текущих явлениях. Это позволяет планировать мероприятия по обеспечению безопасности заранее и повышать эффективность реагирования на угрозы, а также снижать величину ущерба.

Как было сказано ранее суть работы видеоаналитики заключается в получении данных из последовательности изображений, поступающих в режиме реального времени или из архивных записей. Программное обеспечение, выполняющее данную функцию, должно функционировать на какой-либо аппаратной части. Таким образом, в зависимости от того, где осуществляется анализ изображений возможны три варианта построения СОТ с видеоаналитикой, когда обработка осуществляется на видеосервере, видеорегистраторе и видеокамере.

При использовании видеоаналитики на видеосервере на нем устанавливается специализированное ПО, выполняющее различные функции анализа изображений. Это может быть распознавание государственных регистрационных знаков транспортных средств, обнаружение оставленных предметов и т.д. В таком варианте построения возможно масштабирование системы (увеличение количества видеокамер) и расширение выполняемых функций при появлении новых задач путем установки дополнительных программных модулей того же или другого производителя. При необходимости видеоинформация и результат ее обработки могут быть получены удаленно через программу-клиент. При таком варианте построения системы возможности наиболее широки, так как может быть использован видеосервер с достаточно большой производительностью. Обязательным условием нормального функционирования такой системы является обеспечение достаточной пропускной способности каналов связи между видеокамерами и видеосервером. Очевидно, что при увеличении количества видеокамер, нагрузка увеличивается не только на видеосервер, но и на каналы связи.

При использовании видеоаналитики на видеорегистраторе DVR (digital video recorder – цифровой видеорегистратор) или NVR (network video recorder – сетевой видеорегистратор) обработка изображений осуществляется встроенным ПО. Набор функций в этом случае определяется моделью видеорегистратора, однако у большинства производителей этот набор приблизительно одинаковый. Добавление новых функций оперативно путем установки новых программных модулей невозможно. Для этого требуется модернизация встроенного ПО видеорегистратора, что требует затрат времени и должно быть оправдано для большинства потребителей. Алгоритмы видеоаналитики в таком варианте построения более просты, что обусловлено гораздо меньшей производительностью процессоров видеорегистраторов по сравнению с производительностью процессоров видеосерверов. Примерами таких алгоритмов могут служить обнаружение движения в кадре, пересечение линии, поиск лица в кадре и другие. Использование видеоаналитики на видеорегистраторе целесообразно в случае сравнительно небольшого количества видеокамер при фиксированном наборе простых функций. Видеоинформация в такой системе хранится в самом видеорегистраторе и может быть получена удаленно через программу-клиент.

При использовании видеоаналитики на видеокамере обработка изображений осуществляется встроенным ПО видеокамеры. Наиболее широкими возможностями в силу принципа работы обладают цифровые (IP) видеокамеры. Однако и в аналоговых видеокамерах реализуются простейшие алгоритмы. К ним можно отнести простейший детектор движения в кадре. Весь кадр разделяется на фиксированное количество фрагментов и в настройках камеры задается регион интереса (ROI – region of interest), то есть часть кадра, в которой будет детектироваться движение. Кроме того, задается уровень чувствительности в условных единицах, что позволяет игнорировать шумы на изображении и другие изменения изображения, не связанные с движением объектов. Как и в случае с видеоаналитикой на видеорегистраторе в таком варианте построения системы набор функций меньше по сравнению с видеоаналитикой на видеосервере. Достоинства и недостатки аналогичны системам на видеорегистраторе. Отдельно в качестве преимущества стоит отметить более низкие требования к пропускной способности каналов связи, так как вся обработка происходит в видеокамере, а на автоматизированное рабочее место (АРМ) выводится только результат. Кроме того, снижаются требования к производительности видеосервера при его использовании. Видеоинформация в такой системе хранится в самой видеокамере и может быть получена удаленно через программу-клиент.

В некоторых системах используется гибридный вариант, представляющий собой сочетание видеоаналитики на видеокамере и видеосервере. Видеокамера осуществляет предварительную обработку

изображений, а видеосервер осуществляет большую часть вычислений и выполняет заданные функции. Например, при идентификации личности по изображению лица видеокамера осуществляет поиск лиц в кадре и передает их изображение по каналу связи видеосерверу, а он уже проводит идентификацию. В такой структуре построения системы снижается нагрузка на каналы связи и видеосерверы, что позволяет одному серверу осуществлять обработку изображений от большего числа видеокамер. В то же время использование видеокамер со встроенной видеоаналитикой приводит к повышению стоимости системы.

В рамках стандартизации в области информационных технологий в 2020 году был принят первый в истории стандарт ГОСТ Р 59385-2021 Информационные технологии (ИТ). Искусственный интеллект. Ситуационная видеоаналитика. Термины и определения, посвященный применению искусственного интеллекта для ситуационной видеоаналитики. Данный нормативный документ является первым в группе стандартов, устанавливающих нормативные требования в области ситуационной видеоаналитики. Они будут регламентировать эксплуатационные характеристики, методики испытаний и оценки качества и требования к размещению оборудования технических систем интеллектуального видеонаблюдения.

Видеоаналитика может выполнять следующие функции:

1. Обнаружение движения в кадре.
2. Пересечение линии в заданном направлении.
3. Перемещение в/из заданной области.
4. Обнаружение оставленных или пропавших предметов.
5. Распознавание лица человека.
6. Обнаружение праздношатания (бесцельного поведения).
7. Трекинг объектов (построения траектории движения и сопровождение объекта).
8. Распознавание государственных регистрационных знаков транспортных средств, в том числе железнодорожного транспорта.
8. Обнаружение саботирующих действий (перекрытие или засветка объектива, поворот видеокамеры и т.д.).
9. Улучшение качества изображения.

Перечисленные выше функции можно считать базовыми, которые в настоящее время реализованы практически у каждого разработчика видеоаналитики. Однако иногда могут возникать нетиповые задачи, обусловленные какими-либо потребностями. Например, с появлением короновирусной инфекции COVID-19 возникла потребность в обнаружении в кадре людей, не имеющих на лице медицинских масок. Другим примером является обнаружении на строительной площадке людей не имеющих защитных касок.

На объектах информатизации ОВД с успехом могут применятся все вышеперечисленные функции видеоаналитики. Наибольший интерес представляет распознавание лица человека. Данная функция может использоваться при осуществлении контроля и управления доступом на входе в подразделение или в служебные помещения, а также в процедуре аутентификации на рабочих компьютерах.

Распознавание лиц – практическое приложение теории распознавания образов, в задачу которого входит автоматическая локализация лица на неподвижном или движущемся изображении и, в случае необходимости, идентификация личности по характерным параметрам лица. Распознавание лиц людей и определение личности человека – одна из самых востребованных функций видеоаналитики, которая используется практически во всех современных системах безопасности. Распознавание личности по лицу основано на его уникальных параметрах. На лице имеется несколько характерных точек (рис. 8), расстояние между которыми индивидуально для каждого человека подобно папиллярному узору. Доказано, что эти расстояния практически не изменяются в течении всей жизни человека.

Некоторые функции видеоаналитики стали возможны благодаря достижениям в математике, развитию информационно-телекоммуникационных технологий и средств вычислительной техники. Существует ряд функций, реализуемых при использовании нейросетей. Нейросети получили широкую известность с 2012 года. С этого времени всё больше компаний, как известных, так и начинающих, стали широко использовать технологию нейросетей для точного и достоверного распознавания изображений.

Для решения сложных задач видеоаналитики в настоящее время используются нейросети с глубоким обучением DNN (Deep Neural Network), или просто глубокие нейросети.

Глубокие нейросети используются для создания систем, которые могут распознавать объекты и их свойства из объёмных массивов неразмеченных данных. В последнее время для целей глубокого обучения нейросетей все большее применение находят графические процессоры GPU, которые позволяют обучить огромные массивы данных за относительно короткое время. Современные алгоритмы распознавания превосходят по точности, существовавшие 20-25 лет назад примерно на два порядка.

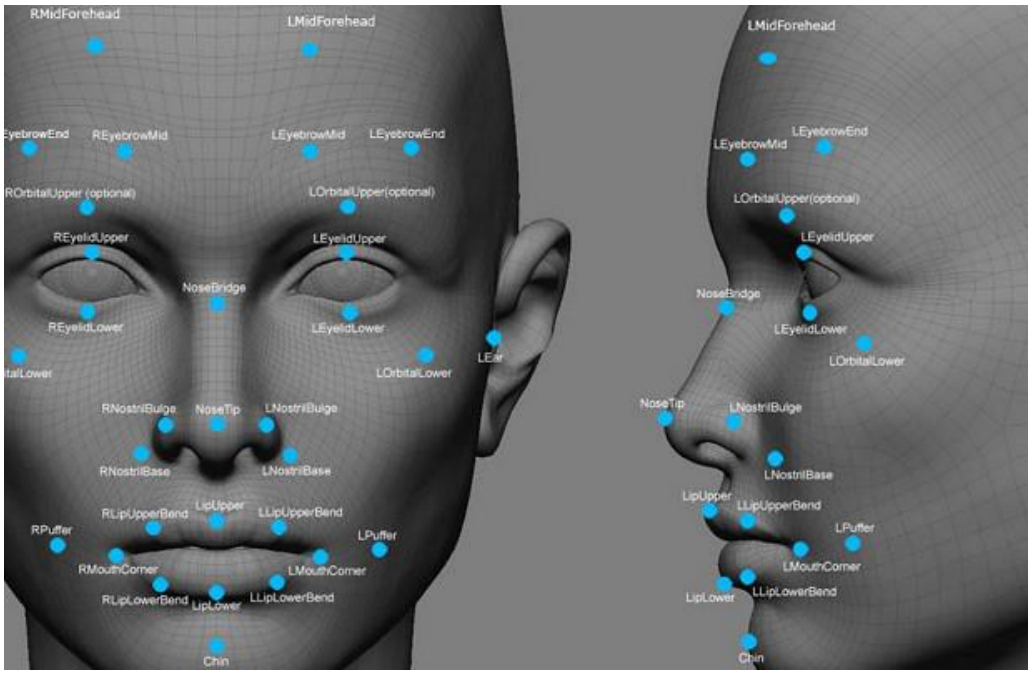

Рис. 8. Расположение опорных (реперных) точек на лице человека

Модели на основе DNN используются для распознавания образов «на лету», в тех случаях, где скорость распознавания очень важна для того, чтобы оперативно выполнить какие-то действия. Однако время обучения может быть значительным. Поэтому, стандартные DNN не всегда удовлетворяют требованиям задержки для некоторых приложений реального времени. Тем не менее хорошо «обученные» DNN могут иметь высокую точность распознавания образов, что очень важно для развития видеонаблюдения.

На рис. 9. показана структура системы видеоаналитики с нейросетью DNN.

Некоторое число n камер следят за определённой областью с целью отслеживания траекторий движения людей и объектов. Нейросеть DNN предварительно обучена распознаванию объектов, определению направления и скорости их движения. На основании этой информации осуществляется анализ характеристик объекта (например, тип и марка транспортного средства, распознавание лиц людей и пр.).

Это может быть сложной задачей, особенно в условиях ограниченности наличных вычислительных ресурсов. Технология очистки данных на основе взаимоотношений RelDC (Relationship-Based Data Cleaning) может повысить качество распознавания, даже в условиях видео не очень высокого качества.

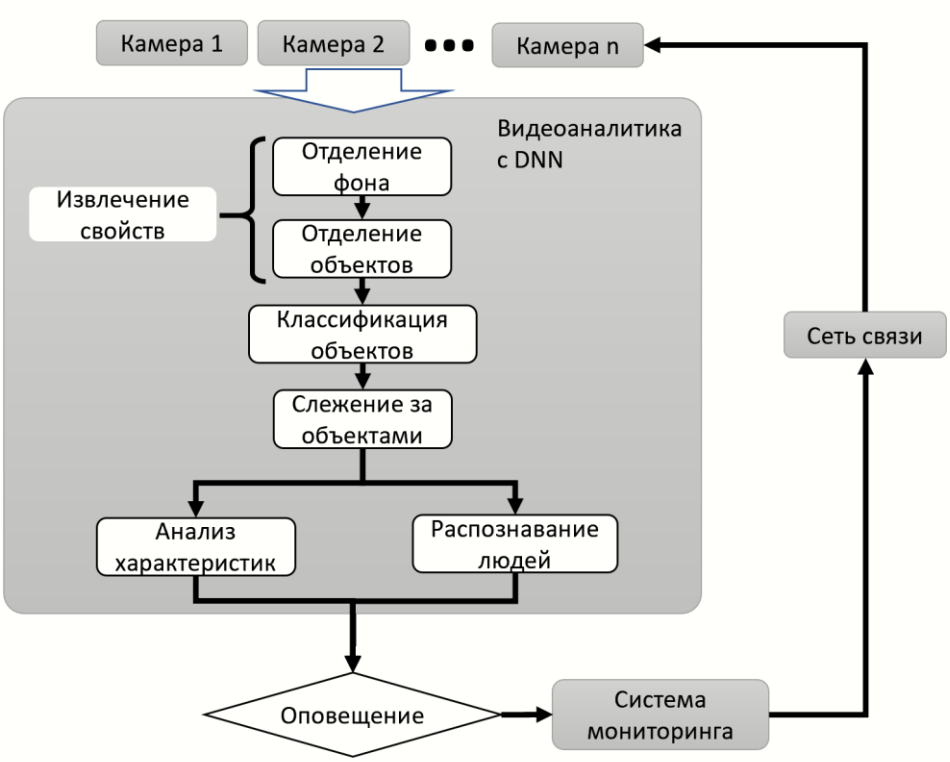

Рис. 9. Структура видеоаналитики с нейросетью DNN

Обычные нейросети состоят из взаимосоединённых вычислительных узлов, называемых нейронами, каждый из который активирует узлы соседнего слоя с установленным весом (величиной) сигнала. Активация начинается на входных нейронах, и затем внутренние «слои» нейронов активируются под воздействием присоединённых к ним нейронов в соответствии с коэффициентами передачи сигнала. Обычные нейросети работают с использованием простого механизма распространения сигнала со входа на выход и имеют не больше 2-3 внутренних слоёв нейронов (рис. 10).

В зависимости от числа скрытых слоёв нейронов для обучения, нейросети классифицируются как «мелкие» (shallow) и «глубокие» (deep), DNN. Мелкие нейросети обычно содержат 1-3 скрытых слоя, в то время как число слоёв в глубоких сетях DNN – от трёх и более. Увеличение числа слоёв повышает эффективность обучения нейросети и точность распознавания образов. DNN могут иметь различную сетевую архитектуру, «модель» (model), которая также существенно влияет на процесс обучения.

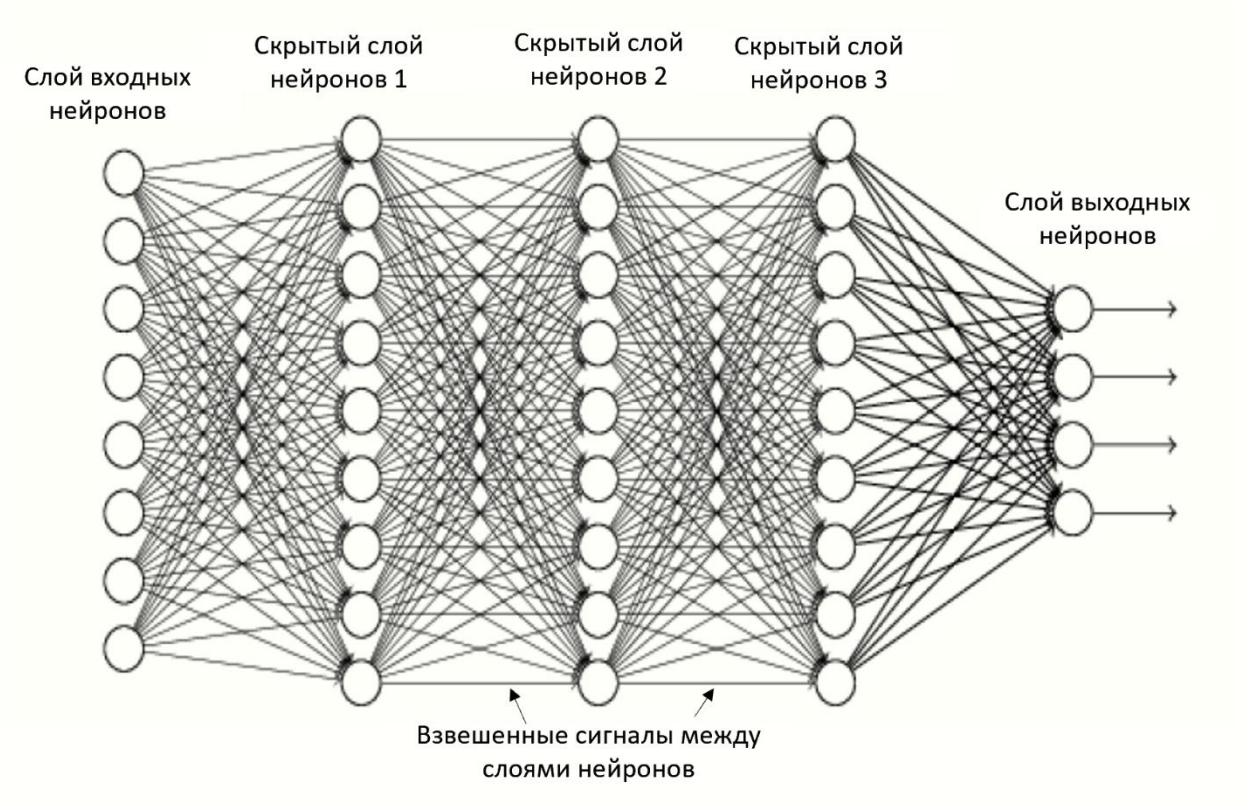

Рис. 10. Нейросеть с тремя скрытыми слоями

Глубокое обучение DL (Deep Learning), как разновидность машинного обучения ML (Machine Learning), использует различные алгоритмы для обработки данных и имитации процесса мышления, чтобы делать различные умозаключения, заключающиеся в распознавании объектов и их поведения. При этом становится возможным распознавать рукописный текст (даже в том случае, если DNN никогда раньше не «видела» почерк данного человека), понимать живую речь (без необходимости предварительной биометрии голоса), и распознавать различные объекты, например, класс «животные», а внутри него – подклассы: «собака», «кошка», «корова» и пр.

Информация в DNN передаётся и обрабатывается последовательно со слоя на слой, когда выходной сигнал после обработки в нейроне предыдущего слоя служит входным сигналом для всех, либо части нейронов последующего слоя, причем сила величина (амплитуда) сигнала определяется «весом» данного линка от нейрона предыдущего слоя к нейрону следующего слоя.

В зависимости от получаемого результата на выходе слоя выходных нейронов, может производиться последовательная коррекция весов отдельных линков между нейронами соседних слоёв. Этот итерационный процесс коррекции весов линков называется «обучением» (Learning) нейросети.

ЗАКЛЮЧЕНИЕ

Использование телевизионных изображений, то есть изображений, полученных с охраняемого объекта или территории на расстоянии, является эффективным способом защиты жизни и здоровья людей, материальных средств, окружающей среды от поражающих факторов пожара, а также способом надежно аутентификации при осуществлении пропускного режима на объекте или при предоставлении доступа к ресурсам информационных систем. Кроме того, одно и то же изображение может быть использовано и для обнаружения иных событий, например, проникновения (попытки) на охраняемый объект (территорию), оставление или пропажа предметов, движение в зоне интереса с предельной скоростью и др. Такие возможности обусловлены высокой информативностью изображения. На приемной стороне системы охранного телевидения наблюдатель получает информацию о количестве и пространственном расположении предметов, их цвете, форме и размерах, перемещении друг относительно друга. Все это в конечном счете позволяет получить комплексное представление о ситуации на объекте.

Дополнительные возможности систем охранного телевидения появляются при использовании высокопроизводительных ЭВМ для более детальной обработки изображений. Это позволяет не только автоматизировать процесс анализа изображений, снизив тем самым нагрузку на оператора, но и получить ряд новых функций. Стоит отметить, что процесс решения задач обнаружения, классификации и идентификации событий является достаточно затратным с технической точки зрения. Это связано с большим объемом информации, заключенном в изображении, и сложностью математического описания происходящих событий в кадре. На текущий момент данная задача достаточно успешно решена рядом отечественных и зарубежных разработчиков, однако абсолютный предел не достигнут и имеются пути совершенствования. Одним из направлений является увеличение вероятности обнаружения и снижение количества ложных тревог, а также повышение помехоустойчивости системы при работе в различных условиях.

В основе алгоритмов видеоаналитики лежат определенные математические модели – нейронные сети. Нейронные сети, обученные на больших объемах данных, способны не только выполнять задачи обнаружения, классификации и идентификации событий, зафиксированных объективами средств видеонаблюдения, но и прогнозировать дальнейшее развитие ситуации. Системы охранного телевидения с функцией видеоаналитики позволяют в разы сократить время обнаружения чрезвычайных ситуаций, что является их основным преимуществом.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Конституция РФ [Электронный ресурс]: принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс».
2. О полиции [Электронный ресурс]: федер. закон Российской Федерации от 7 февраля 2011 г. № 3-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».
3. О безопасности [Электронный ресурс]: федер. закон Российской Федерации от 28 декабря 2010 г. № 390-ФЗ. Доступ из справ.- правовой системы «КонсультантПлюс».
4. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: федер. закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
5. О государственной тайне [Электронный ресурс]: Закон Российской Федерации от 21 июля 1993 г. № 5485-1 (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».
6. О персональных данных [Электронный ресурс]: федер. закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ (ред. от 31 декабря 2017 г.). Доступ из справ.-правовой системы «КонсультантПлюс».
7. Об информации, информационных технологиях и защите информации [Электронный ресурс]: федер. закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
8. Об организации предоставления государственных и муниципальных услуг: федер. закон Российской Федерации от 27 июля 2010 г. № 210-ФЗ // СЗ РФ. 2010. № 31. Ст. 4176. Об электронной подписи [Электронный ресурс]: федер. закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
9. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: Указ Президента РФ от 9 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс».
10. Вопросы организации информационно-аналитической работы в управленческой деятельности органов внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 26 сентября 2018 г. № 623. Доступ из справ.-правовой системы «КонсультантПлюс».
11. Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 31 декабря 2013 г. № 1040. Доступ из справ.-правовой системы «КонсультантПлюс».

12. ГОСТ Р 52551-2016 Системы охраны и безопасности. Термины и определения.

13. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

14. ГОСТ Р 59385-2021 Информационные технологии (ИТ). Искусственный интеллект. Ситуационная видеоаналитика. Термины и определения.

Основная литература:

1. Информационные технологии управления и организация защиты информации: курс лекций / В. А. Апульцин, Ш. Х. Гонов, В. Н. Лебедев, В. Ю. Петрова. – Москва : Академия управления МВД России, 2021. – 72 с.

2. Информационные технологии в управлении и организация защиты: учебник / В. В. Баранов и др.; под ред. И. В. Горошко. Москва: Академия управления МВД России, 2018.

3. Информационные технологии в управлении органами внутренних дел: учебник / В. В. Баранов и др.; под ред. И. В. Горошко. Москва: Академия управления МВД России, 2015.

4. Лукашов Н. В., Лебедев В. Н., Макаров В. Ф. Информатизация и информационная безопасность органов внутренних дел: курс лекций. Москва: Академия управления МВД России, 2012. Торопов Б. А., Апульцин В. А.

5. Технологии многокритериального оценивания результатов деятельности территориальных органов МВД России на региональном уровне: учебное пособие. Москва: Академия управления МВД России, 2016. Защита информации: учебник в 2-х ч. / В. Н. Лебедев и др.; под ред. В. И. Кирина. Москва: Академия управления МВД России, 2013.

6. Ворона В.А., Тихонов В.А., Митрякова Л.В. Теоретические основы обеспечения безопасности объектов информатизации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2016. – 304 с.: ил.

7. Manyika J. Open Data: Unlocking Innovation and Performance with Liquid Information: McKinsey; 2013.

8. Pulse UG. Big data for development: Challenges & opportunities. Nueva York, mayo: Naciones Unidas; 2012.

Электронные ресурсы:

1. Сайт МВД России. URL: http://www.mvd.ru.

2. Сайт ФКУ «ГИАЦ МВД России»

3. Сайт ЦСИ ФКУ «ГИАЦ МВД России»

4. Сайт Единой межведомственной информационно-статистической системы. URL: http://www.fedstat.ru.

Учебное издание

Гречаный Сергей Анатольевич,
Калков Дмитрий Юрьевич,
Меркулова Наталья Ивановна,
Таравков Михаил Владимирович.

СОВРЕМЕННЫЕ ПОДХОДЫ В ПОСТРОЕНИИ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ С ИНТЕГРИРОВАННЫМИ АЛГОРИТМАМИ ВИДЕОАНАЛИТИКИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Методические рекомендации

В авторской редакции.
Компьютерный набор Н.И. Меркулова.
Объем 1 Мб.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53