УДК 004.6:004.75

ВОПРОСЫ ОПТИМИЗАЦИИ ПРОЦЕССОВ РАСПОЗНАВАНИЯ ИСКОМОГО ОБЪЕКТА В ВИДЕОПОТОКЕ С КАМЕР НАБЛЮДЕНИЯ ПУТЕМ ПОВЫШЕНИЯ КРИТЕРИЕВ ГИБКОСТИ И МАСШТАБИРУЕМОСТИ СИСТЕМЫ

Жигалов К.Ю., Аветисян К.Р.

ФГБУН «Институт проблем управления науки В.А. Трапезникова» Российской Академии наук, НОУ ВО «Московский технологический институт», Москва, e-mail: kshakalov@mail.ru

В данной научной статье проанализированы возможности системы видеонаблюдения с функциями 3D-идентификации. Рассмотрены аспекты реализации систем видеонаблюдения с функциями 3D идентификации на основе IP камер с возможностью обработки данных при помощи облачных систем вычисления. С целью актуализации работы самой системы видеонаблюдения и повышения ее работоспособности целесообразным видится перераспределять нагрузку на серверную часть, а именно обработку, хранение, в особенности в вопросах, связанных с реализацией функций видеоаналитики. Видеоаналитика, реализация процедуры которой требует высоких мощностей, целесообразна в рамках серверной части. Использование облачных технологий может повысить эффективность системы видеонаблюдения в целом. Применение облачных технологий при хранении данных предоставляет возможность оператору иметь удаленный доступ. Уделено внимание вопросам оптимизации процессов при распознавании объекта попавшего в зону фиксации, путем повышения гибкости системы видеонаблюдения и её масштабируемости. Результат научно-технического прогресса в области разработки систем распознавания объектов является приоритетным и наиболее значимым направлением в области высоких технологий. Уровень решений, который принимается по вопросам идентификации объектов, отражен не только в рамках научных форумов и конференций международного уровня, но и проектами реализуемыми в рамках крупных компаний и стран.

Ключевые слова: самомодификация, видеонаблюдения, облачные технологии, IP-камеры, распознавание объектов, 3D, видеоаналитика

THE ISSUES OF OPTIMIZATION OF PROCESSES OF RECOGNITION OF THE DESIRED OBJECT IN THE VIDEO STREAM FROM SURVEILLANCE CAMERAS BY INCREASING THE CRITERIA OF FLEXIBILITY AND SCALABILITY

Zhigalov K.Yu., Avetisyan K.R.

V. A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, PEI HE Moscow Technological Institute, Moscow, e-mail: kshakalov@mail.ru

In this research article analyzed the possibility of video surveillance system with functions of 3D-ID. The aspects of the implementation of video surveillance systems with 3D identification functions based on IP cameras with the ability to process data using cloud computing systems are considered. In order to update the operation of the video surveillance system and improve its efficiency, it seems appropriate to redistribute the load on the server part, namely processing, storage, especially in matters related to the implementation of video Analytics functions. Video Analytics, the implementation of which requires high capacity, is appropriate within the server part. The use of cloud technologies can increase the efficiency of the video surveillance system as a whole. The use of cloud technologies in data storage allows the operator to have remote access. Attention is paid to the optimization of processes in the recognition of the object caught in the fixation zone, by increasing the flexibility of the video surveillance system and its scalability. The result of scientific and technological progress in the development of object recognition systems is a priority and the most significant, the level of decisions that is taken on the identification of objects is raised not only in the framework of scientific forums and conferences of the international level, but also when considering the above direction of large companies and countries.

Keywords: modernization, video surveillance, cloud technologies, IP-cameras, object recognition, 3D, video-analytics

Распознавание оптических образов человека, полученных с видеокамер различного типа в режиме реального времени, до сих пор является одной из сложнейших и важнейших задач. На сегодняшний день задачи по распознаванию лиц актуальны и имеют большее количество готовых решений.

Цель данной работы отражена в проведении анализа критериев, при соблюдении которых система видеонаблюдения может проводить функция 3D-идентификацию лиц. Разработка программного обеспечения, реализующего функции идентификации объектов, попавших в зону фиксации, с последующей обработкой массивов данных. Задачи системы распознания в целом состоят в сборе обработке и предоставлении статистической информации конечному клиенту для работы с итоговым массивом данных.

Основные виды систем видеонаблюдения

В настоящее время в системах видеонаблюдения с функциями идентификации

реализованы функции, по которым и производится идентификация попавших в зону фиксации объектов, таких как: определение лица/лиц на фотографии; сопоставление лиц с фотографии с базой данных; поиск человека из базы на фотографии; определение параметров лица (определение глаз, бровей, носа, рта); группирование лиц (легкий поиск, сортировка и отслеживание). Продумывалась серверная составляющая аппаратно-программного комплекса, способного принимать информацию, проводить ее сбор и обработку. Коммуникация между конечным устройством и вычислительными ресурсами осуществляется непосредственно через сеть [1]. Современная сетевая инфраструктура (как проводного, так и беспроводного типа) способна обеспечить необходимую скорость передачи данных.

Основные группы камер исследуемых систем видеонаблюдения:

– инфракрасные;

– стандартные.

Инфракрасные камеры позволяют определять параметры человека в условиях плохой видимости (например, на улице в темное время суток). Кроме того, инфракрасные камеры на аппаратном уровне находят и выделяют элементы лица и части тела людей. Стандартные камеры позволяют хорошо определять параметры человека в хорошо освещенных помещениях или в дневное время суток. Условно, камеры можно поделить на следующие:

1. WEB-камеры (хорошо передают параметры человека на расстоянии до 3 метров, их возможно использовать в рекламных конструкциях в переходах, на кассах супермаркетов, у входов в различные заведения и общественном транспорте);

2. IP камеры (хорошо передают параметры человека на расстояниях до 30–35 метров, что позволяет их использовать на открытых местностях).

Использование стандартов Ethernet (Wi-Fi – при беспроводном и FTP/UTP – при проводном виде соединения) при коммутации камер вносит некоторые затруднения, дело в том, что практически все компьютеры имеют, как правило, один сетевой интерфейс, что не позволит ему подключить одновременно несколько камер и доступ в интернет. В связи с чем в стандартную конфигурацию конечного устройства при таком варианте коммутации необходимо включить Wi-Fi роутер.

К Wi-Fi роутерам предъявляется ряд требований:

– поддержка передачи данных стандарта 802.11 n или выше (для случаев коммутации беспроводных камер и микрокомпьютера);

– наличие не менее трех портов Ethernet (для случаев коммутации проводных камер и микрокомпьютера);

– наличие порта (для предоставления доступа в интернет конечного устройства);

– и др.

Следует отметить, что при использовании беспроводного метода коммутации целесообразно помнить о мерах безопасности, так как будет использоваться открытый канал связи. Данные с видеокамер поступают в специализированное программное обеспечение, где блоки данных разбиваются на части и проводится процедура видео аналитики [2].

Все описанное выше записывается в лог файл системы и отправляется на соответствующий WEB-сервер для дальнейшей обработки и исследований. На данном этапе, система фиксирует и сохраняет данные с видео потока в виде изображений в БД с целью последующего проведения сравнительного анализа. По завершении пилотных исследований данные с систем видеонаблюдении сохранятся.

Отправка данных на веб-сервер позволяет не тратить ресурсы на хранение и передачу по сети информации и осуществлять ее обработку централизованными методами. Что касается технической составляющей, то система построена по клиент-серверной архитектуре, где все операции по хранению данных, распределению изображений возложены на сервер, размещенный в среде глобальной сети. Получение данных с видеокамер, первичная обработка и показ видеоконтента распределен на клиента, который может иметь кроссплатформенное программное обеспечение. Был определен стандартный конструктивный комплект оборудования единичной станции: IP-видеокамера; блок питания; компьютер управления системой, специализированное программное обеспечение. Комплектация конкретного комплекса может несколько отличаться за счет интегрированных систем.

В рамках проведения исследования было выявлено отсутствие существующих систем распознавания с открытым кодом для инфракрасных камер, в связи с чем было принято решение разработать свою собственную систему на базе алгоритма и SDK для 3D камер, а далее провести корректировку алгоритма.

Создание и корректировка ПО системы видеонаблюдения с функцией 3D-идентификации на базе алгоритма SDK

Для начала мы создадим объект конфигурации и сформируем обработчик ошибок:

Объект конфигурации

```
PXCFaceConfiguration* faceCfg = faceModule->CreateActiveConfiguration();
if (faceCfg == NULL)
assert(faceCfg);
return;
```

Выполним процедуру инициализации и осуществим настройки стрима:

Инициализация и настройка стрима

```
faceCfg->SetTrackingMode(FaceTrackingUtilities::GetCheckedProfile(dlgWnd));
faceCfg->ApplyChanges();
PXCCapture::Device::StreamProfileSet profile;
If (FaceTrackingUtilities::IsModuleSelected(dlgWnd, IDC_PULSE) &&
!FaceTrackingUtilities::GetPlaybackState(dlgWnd))
memset(&profile, 0, sizeof(profile));
profile.color.imageInfo.height = 720;
profile.color.imageInfo.width = 1280;
cMgr->FilterByStreamProfiles(&profile);
```

Зададим функции, отвечающие за обработку, инициализацию, получение структуры сессии и настройку формата записи данных:

Функции обработчика сессии

```
if (sMgr->Init() < PXC_STATUS_NO_ERROR)
cMgr->FilterByStreamProfiles(NULL);
if (sMgr->Init() < PXC_STATUS_NO_ERROR)
FaceTrackingUtilities::SetStatus(dlgWnd, L»Init Failed», statusP);
faceCfg->Release();
sMgr->Close();
sMgr->Release();
return;
```

Функции инициализации сессии

```
PXCCapture::DeviceInfo devInfo;
sMgr->QueryCaptureManager()->QueryDevice()->QueryDeviceInfo(&devInfo);
CheckForDepthStream(sMgr, dlgWnd);
FaceTrackingAlertHandler alertHandler(dlgWnd);
if (FaceTrackingUtilities::GetCheckedModule(dlgWnd))
faceCfg->detection.isEnabled = FaceTrackingUtilities::IsModuleSelected(dlgWnd,

IDC_LOCATION);
faceCfg->landmarks.isEnabled = FaceTrackingUtilities::IsModuleSelected(dlgWnd,
IDC_LANDMARK);
faceCfg->pose.isEnabled = FaceTrackingUtilities::IsModuleSelected(dlgWnd, IDC_POSE);

FaceTrackingUtilities::IsModuleSelected(dlgWnd, IDC_PULSE) ? faceCfg->QueryPulse()-
Enable() :
faceCfg->QueryPulse()->Disable();
if (FaceTrackingUtilities::IsModuleSelected(dlgWnd, IDC_EXPRESSIONS))
faceCfg->QueryExpressions()->Enable();
faceCfg->QueryExpressions()->EnableAllExpressions();
else
faceCfg->QueryExpressions()->DisableAllExpressions();
faceCfg->QueryExpressions()->Disable();
if (FaceTrackingUtilities::IsModuleSelected(dlgWnd, IDC_RECOGNITION))
faceCfg->QueryRecognition()->Enable();
faceCfg->EnableAllAlerts();
faceCfg->SubscribeAlert(&alertHandler);
```

В ходе проведения опыта по установлению полезной дистанции (зоны наблюдения) при изучении наблюдаемого объекта-лица было установлено, что лишь существенное отклонение анализируемой поверхности (лица) приводит к сложностям в фиксации и последующей идентификации попавшего в зону контроля системой видеонаблюдения. Представлены (рис. 1, 2) кадры фиксации лица и построение точечной трехмерной модели с сохранением параметров, с последующей идентификацией объекта при попадании его в зону фиксации системы видеонаблюдения.

Вывод: идентификация исследуемого объекта, а именно изображение лица в форматах «профиль» и «анфас» – при данных углах ротации (от 0 до 70 градусов по оси абсцисс и от 0 до 50 градусов по оси ординат), а также удаленности от системы видеонаблюдения от 0 до 1 метра – возможна и может быть проведена корректно.

Исходя из вышеперечисленного эффктивность установки данного типа систем видеонаблюдения отражена в местах проведения досмотровых мероприятий и контрольно-пропускных пунктах.

Следующие изображения (рис. 3, 4) отображают ротацию объекта, при которых процедура 3D-идентификации осуществляется некорректно.

Вывод: игнорирование вышеуказанных пределов не позволяет провести изначально фиксацию объекта и впоследствии идентифицировать его.

Мы видим, что лишь значительные развороты головы, которые неестественны в штатных случаях у людей при появлении в таких зонах контроля, как СКУД и другие, фокус внимания ориентирован по направлению движения, и скорость передвижения не более 1–3 км/ч, что позволяет многократно произвести фиксацию исследуемого объекта.

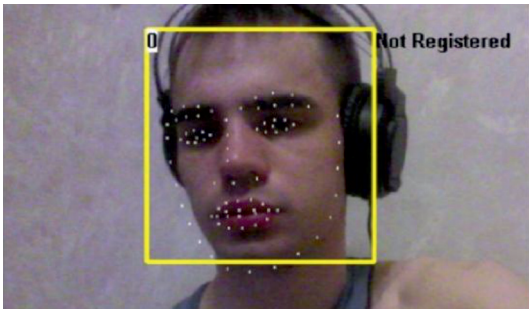

Рис. 1. Анфас

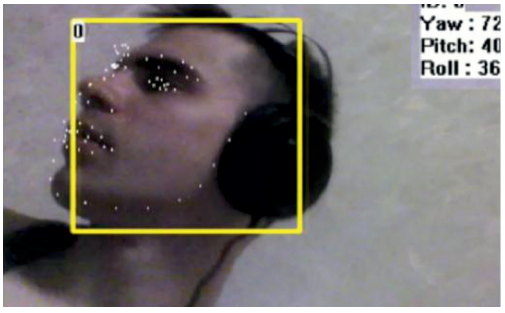

Рис. 2. Профиль

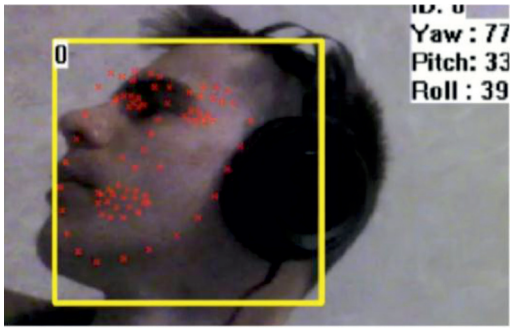

Рис. 3. Анфас

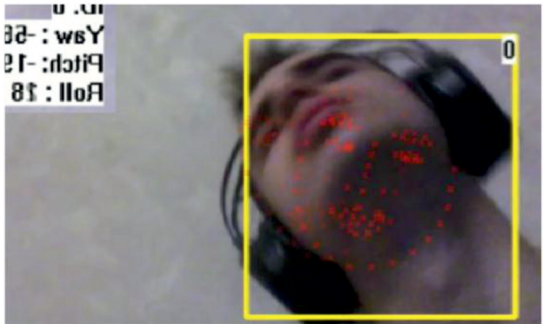

Рис. 4. Профиль

Выведение функций записи структуры

Функции записи струткуры и обновления событий

```
faceCfg->ApplyChanges(); //
FaceTrackingUtilities::SetStatus(dlgWnd, L»Streaming», statusP);
mOut = faceModule->CreateOutput();
bool secondMoreFrame = false;
bool stopPlaying = false;
ResetEvent(render->GetRenderingFinishedSignal());
```

Выставление объектов и обработчика кадров

Процедура выставления нового объекта

```
render->SetSenseManager(sMgr); //
render->SetNumberOfLandmarks(faceCfg->landmarks.numLandmarks);
render->SetCallback(render->SignalProcessor);
кулбек
if (!isStopped)
while (true)
```

Обработчик падений

```
if (sMgr->AcquireFrame(true) < PXC_STATUS_NO_ERROR) //
stopPlaying = true;
if (secondMoreFrame)
WaitForSingleObject(render->GetRenderingFinishedSignal(), INFINITE);
```

Освобождаем ресурсы

```
if (stopPlaying || isStopped) // ибо утечки
if (isStopped)
sMgr->ReleaseFrame();
if (stopPlaying)
PostMessage(dlgWnd, WM_COMMAND, ID_STOP, 0);
break;
```

Выведение функций регистрации пользователя и обновления кадра

Регистрация пользователя

```
if (faceCfg->QueryRecognition()->properties.isEnabled) //
if (mRegFlag)
reg();
if (mUnregFlag)
unreg();
удаление кадра
sMgr->ReleaseFrame();
```

Обновление кадра, объект обработанного кадра

```
mOut->Update(); //
PXCCapture::Sample* sampleMgr = sMgr->QueryFaceSample(); //
secondMoreFrame = true;
if (sampleMgr != NULL)
DWORD dwResult;
dwResult = WaitForSingleObject(ghMutex, INFINITE);
if(dwResult == WAIT_OBJECT_0)
```

Формируем кадр для окна программы

```
render->DrawBitmap(sampleMgr, faceCfg->GetTrackingMode() == PXCFaceConfigurat
on::FACE_MODE_IR);
```

Выставляем и запрашиваем отрисовщик на обновление

```
render->SetOutput(mOut);
render->SignalRenderer(); //
if(!ReleaseMutex(ghMutex))
throw std::exception(«Failed to release mutex»);
return;
```

В ходе разработки прототипа комплекса были отлажены основные схемотехнические решения устройства, в дальнейшем планируется продолжить работу по оптимизации схемотехнической части, а также – максимальной унификации аппаратной составляющей системы. Отдельной важной задачей является выработка предложений по созданию баз данных для обучения искусственного интеллекта типам и стилям одежды.

Также в рамках работы была разработана методика и созданы алгоритмы и программные коды распознавания лиц и их параметров для инфракрасных трехмерных камер. Подготовлена и отправлена заявка на регистрацию программного средства распознавания и сопоставления лиц для инфракрасных 3D камер.

Преимущества IP-видеокамер в системах видеонаблюдения

На сегодня контроль видеопотока является одним из актуальных направлений при построении систем видеонаблюдения. Рассмотрим преимущества IP-видеокамер над их аналоговыми в вопросах безопасности. Обеспечение безопасности данных при построении системы видеонаблюдения с возможностью доступа из глобальной сети, кроме как парольной защиты и стандартных процедур настройки маршрутизатора, реализуется посредством криптографических методов средств.

Ввиду чего одним из основных минусов аналоговых камер можно назвать отсутствие шифрования, как аппаратного, так и программного. Поступающий сигнал по коаксиальному кабелю с аналоговой камеры на регистраторе хоть и предоставляет возможность ограничения доступа к регистратору посредством парольной защиты, однако сам канал передачи данных остается незашифрованным. Так как канал связи не защищен, сохранность данных остается под вопросом. В цифровых IP-камерах эта проблема решена с помощью цифровых водяных знаков и любую подмену можно тут же обнаружить, поэтому угрозу перехвата и подмены картинки при использовании цифровых IP-видеокамер можно исключить. При подключении в системах видеонаблюдения IP-камер надежную защиту обеспечит: установление маршрутизатора на вход с заданными параметрами доступа; с целью защиты данных на сервере от несанкционированного доступа – реализация процедуры шифрования данных видеопотока [3].

Вариантов кодирования и декодирования данных в системах видеонаблюдения предостаточно. Но, по нашему мнению, ключевым критерием в вопросах обеспечения безопасности посредством шифрования видеопотока и данных в целом необходимо рассмотреть такую процедуру, как самомодификация, с целью дальней интеграции принципов динамического полиморфизма в процесс кодировки и декодирования. Такой приём, как динамическая шифровка (специальная техника, используемая авторами программного обеспечения для повышения уровня крипто-стойкости), используется более современными и совершенными средствами защиты полученных программ. Использующаяся как основная, в обычных навесных протекторах, статическая шифровка в большинстве случаев бесполезна.

При использовании полиморфно сгенерированных «на лету» процедур шифрования, автоматизировать дешифровку (распаковку) программы крайне затруднительно, однако создать такой механизм защиты сложно, что является одним из факторов, затрудняющих распространение полиморфных защитных механизмов (полиморфных крипторов) [4, 5].

Если модификация команд отслеживается, как это выполняется на процессорах семейства, начиная с Pentium, такие действия, как IF, OR, выполняются конвейерно, программная длина равна нулю, что приводит к вызову исключения по выполнению на отладчике в старых защитных механизмах, не учитывающих данную задокументированную особенность поведения конвейера процессора. Код, выполняющий описываемую операцию, на языке программирования С, синтаксически описывается так:

*«void *cat = (void *) dog;»*

Использование технологий облачных вычислений в современных системах видеонаблюдения позволяет получать аудио- и видеоинформацию в режиме реального времени при удаленном администрировании. Это конкурентное преимущество. Развитие облачных вычислений, в особенности применения облачных технологий в системах видеонаблюдения, несмотря на вызовы и риски, является перспективным направлением [6].

При использовании облачных вычислений, клиенты информационных технологий значительно снизят затраты ресурсов на формирование центров обработки данных, приобретение сетевого оборудования, программно-аппаратных комплексов по обеспечению непрерывности и работоспособности всей системы [7].

Посредством 3D камер приложения могут выполнять распознавание тех или иных

заданных элементов: жестов, анализ лиц, выделение фона, распознавание звуковых сигналов – голоса, синтез голоса, – предоставляя обширный и полезный инструментарий. Основным критерием политики безопасности облачных технологий при обмене данными в системе видеонаблюдения выступает зашифрованный канал.

Самомодификация при достижении криптоустойчивости

Самомодификация как совокупность алгоритмов, заданных администратором, применяется с целью повышения устойчивости к реверс-инжинирингу и ускорения выполнения некоторых участков кода (к примеру, правки адреса и типа перехода «на лету»), или отключения части функционала на время отладки.

Динамическая шифровка сегодня распространена среди наиболее современных и совершенных средств защиты в топологии программных продуктов. Становится ясным, что для создания полного дизассемблированного листинга необходим полностью расшифрованный двоичный код. Кроме этого, отладка с подключением к процессу так же невозможна в том случае, если используется множество антиотладочных приёмов.

В достижении эффективной защиты, реализация функций «crypt» и «decrypt» при обработке данных в облаке, программный код ни на одном из участков не должен быть расшифрован. Расшифровщик должен быть сконструирован так, чтобы было невозможно использовать его вне контекста программы, так как это является простейшей и распространённой уязвимостью [8].

При нахождении точки входа в процедуру расшифровщика, имеется возможность восстановить его прототип – шеллкод, вызываемый динамически или статически полученным на него указателем, после расшифровать весь оставшийся код. В случаях с низким уровнем шифрования данных процесс декодировки может быть представлен в следующем виде: достаточно найти место хранения ключей, либо, при использовании обратимого шифрования, установить алгоритм шифрования (UUEncode, Base64, Rot13) после, выполнить процедуру дешифровки без внесения правок в какие-либо функции [9].

Исходя из вышеперечисленного, можно также утверждать, что при использовании шифрованного видеопотока, защита сети на транспортном уровне по модели OSI и использовании цифровых водяных знаков, третьему лицу (противнику) подменить либо захватить видео из сети будет трудно-реализуемо.

Заключение

Оптимизация процессов распознавания объекта, попавшего в зону фиксации системы видеонаблюдения, проведена корректно, с установлением ключевых критериев: угла отклонения (до 50 градусов), ротации элемента распознавания (до 70 градусов по оси абсцисс и до 50 градусов по оси ординат); а также полезной дистанции, при которой возможен процесс фиксации и распознавания системой видеонаблюдения до 1 м. Исходя из вышеперечисленного актуальность установки данного типа систем видеонаблюдения отражена в местах проведения досмотровых мероприятий и контрольно-пропускных пунктах, игнорирование вышеуказанных пределов не позволяет провести изначально фиксацию объекта и впоследствии идентифицировать его.

В результате проведенных всесторонних исследований был разработан пилотный программный прототип системы, модульного типа по распознаванию лиц и сопутствующих качественных параметров людей, а также отдельных видов одежды и аксессуаров по данным с камер различного типа. Модульность позволяет в дальнейшем применять различные решения для оптимальной работы системы.

На сегодняшний день ведущие компании в сфере разработки систем видеонаблюдения и, в частности, 3D-идентификации: Microsoft, Kairos, Google, NTechlab, OpenNI2, Orbbec, Intel.

Создание высокотехнологичной системы с функциями фиксации поступающих изображений и анализа видеопотока, на базе алгоритма и SDK для 3D камер – приоритетное направление в области науки и техники. Такого рода системы актуальны к внедрению в государственных и коммерческих организациях. Системы 3D идентификации эффективны при выполнении достаточно широкого круга задач: поиск лиц в БД; видеоаналитика и др.

Список литературы

1. Nikulchev E., Ilin D., Biryukov D., Bubnov G. Monitoring of information space for professional skills demand. Contemporary Engineering Sciences. 2016. T. 9. № 14. P. 671–678. DOI: 10.12988/ces.2016.6327.

2. Жигалов К.Ю., Аветисян К.Р. Применение облачных технологий в системах видеонаблюдения // Современные наукоемкие технологии. 2018. № 1. С. 17–21.

3. Kirill Zhigalov, Karen Avetisyan Using cloud computing technologies in IP-video surveillance systems with the function of 3d-object modelling // 7th Seminar on Industrial Control Systems: Analysis, Modeling and Computing. ITM Web of Conferences, ICS 20183 (https://doi.org/10.1051/itmconf/20181802004) P. 02004.

4. Nikulchev E., Pluzhnik E., Biryukov D., Lukyanchikov O., Payain S. Experimental Study of the Cloud Architecture Selection for Effective Big Data Processing. International Journal of Advanced Computer Science and Applications. 2015. № 6. P. 22–26.

5. Nikulchev E., Pluzhnik E., Biryukov D., Lukyanchikov O. Designing applications in a hybrid cloud. Contemporary Engineering Sciences. 2015. T. 8. № 21. P. 963–970. DOI: 10.12988/ces2015.57214.

6. Плужник Е.В., Никульчев Е.В. Функционирование образовательных систем в гибридной облачной инфраструктуре // Известия вузов. Проблемы полиграфии и издательского дела. 2013. № 3. С. 96–105.

7. Никульчев Е.В., Паяин С.В., Плужник Е.В. Динамическое управление трафиком программно-конфигурируемых сетей в облачной инфраструктуре // Вестник Рязанского радиотехнического университета. 2013. № 3. С. 54–57.

8. Pluzhnik E., Nikulchev E., Payain S. Laboratory test bench for research network and cloud computing. International Journal of Communications, Network and System Sciences. 2014. T. 7. № 7. P. 243–247. DOI: 10.4236/ijcns.2014.77026.

9. Pluzhnik E., Nikulchev E., Payain S. Optimal Control of Applications for Hybrid Cloud Services. Conference: 2014 IEEE World Congress on Services (SERVICES), At Anchorage, AK, USA, P. 458–461. DOI: 10.1109/SERVICES.2014.88.