

# ДИСТАНЦИОННОЕ ОБУЧЕНИЕ В СОВРЕМЕННОЙ РОССИИ: РЕАЛИЗАЦИЯ МЕЧТЫ

**В. Антуфьев**  
начальник сектора информационного обеспечения  
ФГНУ «Главный государственный  
экспертный центр оценки образования»

**П**осле выхода статьи о дистанционном образовании в «Алгоритме безопасности» №1 за 2007 год мне позвонили несколько знакомых – коллег из сферы технической безопасности. Повторяя друг друга, они спросили, что за систему мы создали в «Главэкспертцентре» и будем ли показывать ее на выставке MIPS-2007. Значит, задуманного эффекта от неожиданности уже не получится. Приходится признать: в ФГНУ «Главэкспертцентр» создан аппаратно-программный комплекс удаленного контроля учебного процесса «ВиКонт». Основное назначение комплекса, как следует из названия, – контроль прохождения обучающимися аттестаций (тестирований, экзаменов и т.п.) в дистанционном образовании.

Для тех, кто не читал статью в №1 «Алгоритма безопасности», – «краткое содержание предыдущих серий».

Как это ни странно, но в России существует дистанционное образование. Ключевое слово здесь – «существует». Основной пик шума вокруг дистанционных образовательных технологий приходится на конец 90-х годов. Разрушение советского строя повлекло за собой коренную ломку принципов высшей школы. Из «питалища наук» вузы превратились в коммерческие по сути предприятия, вынужденные сами добывать себе средства для существования. В то время дистанционное образование, с точки зрения экономики, казалось решением многих проблем, поскольку снижало себестоимость образовательных услуг более чем на половину. Министерством образования было разрешено проведение масштабного эксперимента по внедрению дистанционных технологий, и, естественно, в эту сферу кинулись все кому не лень. Проблема заключалась в том, что каждый понимал термин «дистанционка» так, как ему заблагорассудится, то есть так, как

удобнее и выгоднее в конкретный момент времени.

Нельзя сказать, чтобы эксперимент закончился безрезультатно. Путем проб и ошибок были найдены основные принципы построения дистанционного учебного процесса, сформулированы критерии создания технических средств.

Но, после того как перестроечная волна схлынула, оказалось, что дистанционное образование не востребовано в той мере, в какой предполагалось. Коммерциализация общества должна была повлечь за собой значительный, в разы, всплеск спроса на услуги дополнительного образования. Главным образом на краткосрочные курсы повышения квалификации и переподготовки специалистов различных отраслей. Наиболее предпочтительным способом получения дополнительного образования являются именно дистанционные образовательные технологии. Но всплеска интереса не произошло. Причина – недоверие к качеству образования, полученного дистанционным методом. А первопричина – отсутствие какой бы то ни было приемлемой системы контроля качества.

Во всем мире качество образования оценивают по выходным результатам. То есть, при поступлении в вуз никого не интересует, сколько уроков в школе прогулял абитуриент Петров и курил ли он на переменах. А вот итоговые оценки в аттестате являются объектом самого пристального изучения.

Теперь возьмем среднестатистического работодателя. Разглядывая диплом об образовании, полученном традиционными методами (очное, заочное, вечернее), он подсознательно видит тишь академических аудиторий, компетентную неподкупную экзаменационную комиссию за столом, покрытым зеленым сукном, и ужас в глазах испытуемого, тянущего экзаменационный билет.

А что он видит в дипломе, в котором

присутствует слово «дистанционное»? Тунеядца, который, развалившись на собственном диване, жмет на кнопки компьютера в окружении вороха справочников и толпы советчиков! Соглашались, картина не очень-то приглядная. Что немаловажно, ту же картину видит потенциальный потребитель образовательных услуг, выбирая способ получения образования. И, как правило, выбирает традиционный метод. Существуют, правда, ситуации, в которых получение образования не выходя из дома и без особого умственного напряжения является предпочтительным, а качество не имеет никакого значения. Но в таких случаях еще проще купить диплом в переходе столичного метро или по объявлению в сети Интернет. Это и дешевле и быстрее, если не учитывать проблемы с законностью подобного мероприятия.

Здесь надо оговорить несколько исключений из общего правила.

Иногда человеку важнее не конечный результат в виде документа о полученном образовании, а объем и качество приобретенных знаний. В этой ситуации включается механизм самоконтроля. Но, согласитесь, все-таки это частный случай.

И, конечно, не следует забывать о корпоративных системах дистанционного образования, получивших в последнее время большое распространение в крупных компаниях по всему миру. Но корпоративная система образования – вещь в себе. И учителя, и ученики являются сотрудниками одной компании, играющими по своим внутренним правилам. Качество обучения напрямую влияет на карьерный рост и зарплату, недостатки образования выявляются сразу же, так что присутствует внутренний контроль. Тем более что образовательный продукт создается, реализуется и используется в замкнутом круге одной организации. Извне мы видим только конечные результаты проводимой работы в виде повышения курса акций, внедрения новых продуктов и технологий и прочих реалий научно-технического прогресса.

Во всех остальных случаях единственным способом повышения доверия к качеству дистанционного образования является внедрение систем удаленного контроля процедуры аттестации обучающегося.

Дистанционное образование – продукт высоких технологий. Основные его отличия от всех прочих видов образования – это упор на самообразование, индивидуальный учебный график и отсутствие физического контакта между учителем и учеником. Исходя из этого, естественно было бы предположить, что системы контроля дистанционного образования должны быть автоматизированными.

Таким образом, мы вплотную подо-

брались к техническим особенностям построения систем удаленного контроля аттестаций – на примере аппаратно-программного комплекса «ВиКонт», естественно.

Я приношу свои глубочайшие извинения за столь длинное вступление, но, согласитесь, когда специалисту по микроконтроллерам говорят о необходимости обработки данных рецепторов в офтальмологии, он спрашивает: «Что такое офтальмология?». Точно так же специалисту по техническим средствам безопасности не надо объяснять, что такое биометрическая идентификация и видеорегистрация. Его интересует, каким местом все это можно прикрутить к дистанционному образованию и зачем это нужно.

Чтобы не заниматься раскручиванием товара без пометки «На правах рекламы», я не буду описывать особенности реализации конкретных участков программного кода, а буду говорить только о принципах построения систем удаленного контроля, попутно объясняя, на основании каких причин выбран тот или иной подход к решению проблемы.

Итак, приступая к моделированию системы удаленного контроля, мы сталкиваемся с ситуацией, совершенно нетипичной для сферы безопасности: необходимостью получения удовлетворительных результатов при полном отсутствии сведений о конфигурации оборудования конечного пользователя.

Все, что нам известно, это то, что в системе существует устройство видеозахвата и подключение к сети Интернет. Кроме того, поскольку стандартом де-факто для операционных систем в России является пока Windows, будем считать, что на компьютере пользователя установлена именно она.

Видимо, имеет смысл ввести для обозначения комплексов такого класса термин «система безопасности бытовой комплектации». Вопрос в том, как с таким классом работать?

У Микеланджело Буонаротти спросили, как он делает свои гениальные скульптуры? Ответ сохранился в веках: «Я беру глыбу мрамора и отсекаю от нее все лишнее». Примерно по такому принципу и проектировался наш комплекс – естественно, не в смысле гениальности, а в смысле «лишнего».

С видеозахватом вроде бы все достаточно понятно. Любая видеокамера, так или иначе подключаемая к компьютеру, будет взаимодействовать с Windows. (Покажите мне производителя, который настолько не любит деньги, что из-за несовместимости драйвера готов потерять 90% рынка сбыта продукта.) Следовательно, огород городить не требуется. Используем вызовы системных функций библиотеки avicap32.dll и получаем картинку, пригодную для дальнейших манипуляций. Проблемы нач-

нутся, когда мы попытаемся определить приемлемое качество картинки. Видеоустройство может иметь как 10-мегапиксельную, так и 100-килопиксельную матрицу, да еще черно-белую. Ну что же, по крайней мере, нам известен нижний порог, а с повышенным качеством изображения мы как-нибудь справимся. Печально вздохнем и пойдем в магазин покупать самую дешевую USB-камеру. Еще лучше – пойти на рынок и покопаться в компьютерных развалах. Там иногда попадается настоящий антиквариат, и нижний порог у нас будет – ниже некуда.

Одной из основных задачей комплекса удаленного контроля является идентификация пользователя. Поскольку комплекс должен функционировать в автоматическом режиме, без использования спецоборудования, речь может идти только о биометрической идентификации по изображению лица. А здесь нас поджидает целый букет проблем. Впрочем, чтобы заранее не пугать читателей, можно сказать, что вся биометрическая идентификация – одна большая проблема.

Исходя из смысла процедуры аттестации обучающегося, нам необходимо сравнить фотографию на документе, удостоверяющем личность (предположительно – общегражданский паспорт), и изображение лица, полученное в режиме реального времени.

И первое, в чем нам необходимо удостовериться, что в объектив видеокамеры нам показывают именно лицо, а не, извините, другую часть тела. То есть необходим модуль детекции ареала лица в контексте изображения.

Те из вас, кто хотя бы раз сталкивался с биометрическими технологиями, наверняка слышали про динамическую библиотеку OpenCV, с открытым исходным кодом. Библиотека служит для анализа и проведения различных манипуляций с изображениями, в том числе и для поиска лица на картинке. Беда в том, что предназначение библиотеки скорее научно-исследовательское, а не практическое. Правда, каждый желающий может поменять библиотеку или ее часть в сугубо утилитарных целях. Применим ее и мы, с некоторыми модификациями.

Для квалифицированного специалиста выделить из библиотеки модули, отвечающие за детекцию лица, не сложно. OpenCV позволяет находить несколько лиц, определять лицо при достаточном больших градусах наклона и поворота головы, в профиль и в фас – правда, и места эти модули занимают немало. Для наших целей мы применим метод забивания гвоздей микроскопом. То есть выбросим все лишнее, оставив только ту часть программного кода, которая отвечает за определение одного лица строго во фронтальной проекции, возможно, с незначительным поворо-

том и наклоном, и намеренно загрубим модуль. Для пользователя не составит труда посидеть несколько секунд неподвижно, глядя прямо в камеру.

В нашем случае скомпилированный модуль занял всего 120 kb, что, согласитесь, не так уж и много для подгружаемой из Интернета библиотеки.

А для того чтобы в корне пресечь ползновения идентифицируемого на свободу передвижения, применим нижеследующий алгоритм.

В окне видеозахвата разместим прямоугольную рамку, пропорциональную длине и ширине странице паспорта. Внутри рамки поместим еще одну, тоже прямоугольную, соответствующую положению фотографии на странице. Предусмотрим детекцию лица только в сегменте, определенном границами второй рамки. И только при определении лица внутри рамки запустим (по команде пользователя или автоматически) процедуру сохранения захваченного изображения.

Страница паспорта нам нужна для определения соответствия данных паспорта введенным пользователем при открытии доступа к комплексу, вот только лицо с этой страницы не подлежит идентификации в связи с крайне низкой детализацией изображения. Но и эта проблема решается. Введем промежуточное звено. Развернем окно видеозахвата до предельных для большинства устройств 600 x 480 пикселей. Вновь создадим в окне рамку, соответствующую размерам фотографии, но уже во все окно. Предложим пользователю поместить паспорт перед объективом так, чтобы максимально точно вписать фотографию в рамку. Снимки одного и того же изображения лица, пусть даже сильно различающиеся по качеству, идентифицируются практически на 100% даже без нормализации изображений.

Итак, мы имеем: изображение страницы паспорта с данными пользователя и изображение лица, гарантированно принадлежащее этой странице. Остается получить реальное изображение лица пользователя, что мы и делаем по уже описанному выше методу. Для увеличения вероятности идентификации можно предусмотреть получение двух, трех и более изображений. Главное – помнить об Интернет-трафике и не переусердствовать.

Следующая проблема – нормализация изображений лица, которая вообще проблемой не является. Наверное, разумно было бы сразу преобразовать изображения в формат PGM (Portable Gray Map). Почему именно PGM? Ну, во-первых, все так делают, только это скорее следствие, а не причина. А во-вторых, формат PGM является яркостной матрицей изображения в чистом виде, максимально пригодной для дальнейших преобразований и биометрических процедур.

Для тех, кто не знаком с этим форматом, я коротко опишу его особенности.

В первой строке заголовка файла формата PGM записывается условное обозначение формата (P5). Далее, с новой строки – ширину картинки в пикселях (например 100), также с новой строки ее высоту, опять с новой строки максимальное значение оттенков серого в картинке (как правило, 255) и, наконец, с новой строки ASCII – символьные обозначения, характеризующие яркость каждого пикселя в картинке, выраженную в порядковом номере символа от 0 (черный) до 255 (белый). Символы записываются в одну строку. Поскольку формат ориентирован на \*nix системы, для переноса строки пользуемся символом возврата (LF), а не переноса каретки (CR). Полную спецификацию и описание модификаций формата вы можете найти в Интернете. Картинка 100 x 100 пикселей занимает ~10 kb. В два-три раза больше, чем GIF или JPEG, но зато в три и более раз меньше, чем BMP.

Увы, ничто не совершенно в этом мире, поэтому добиться идеальной фронтальной проекции лица, без наклонов и поворотов головы, при простой видеосъемке практически недостижимо. Человеку свойственно двигаться. Что говорить, если даже такая организация как НКВД в 1937-ом году не смогла добиться полного ограничения свободы передвижения советских граждан и некоторый их процент так и не попал в тюрьмы и ссылки. А ресурсов и возможностей у НКВД было побольше, чем у нас. Следовательно, без нормализации не обойтись.

Литературы и примеров исходного кода по трансформации изображений существует великое множество, поэтому ограничусь простым перечислением этапов нормализации:

1. Ориентируем на полученные при детекции лица координаты центров зрачков, производим ротацию картинки до расположения зрачков на одной горизонтальной линии.
2. Масштабируем изображение до приведения межзрачкового расстояния к заранее заданной цифре.
3. Регулируем яркость и контрастность изображения.
4. Выделяем контур лица и все, что находится вне этого контура, заменяем нейтральным фоном.

Произведенных манипуляций вполне достаточно для получения приемлемых результатов. Мы использовали для идентификации метод анализа принципиальных (или главных) компонент (РСА), хотя с таким же успехом можно применять любой другой алгоритм. Необходимо помнить, что при настройке параметров идентификации надо делать упор на максимальное снижение количества ложных распознаваний, даже ценой отказа в доступе для части легитимных пользователей. А для того чтобы довести до 100% безошибочность процедуры идентификации, мы прибе-

регли козырной туз в рукаве.

Если вы помните, на заре компьютеризации существовала такая специальность, как оператор ЭВМ. Специалисты этого профиля пробивали дырки в перфокартах, нажимали на кнопки, сматывали в рулоны ленты распечаток и выполняли еще множество столь же необходимых функций. Так вот, если разнести процедуры проверки соответствия пользователя его паспортным данным и непосредственно тестирования по времени, как минимум, на несколько дней, а принятие окончательного решения по сомнительным случаям доверить оператору ЭВМ, то мы как раз и получим свои возжеланные 100% идентификации пользователя по фотографии в паспорте. А при проведении самого тестирования будем сравнивать изображение пользователя с его же снимком из базы данных, полученном всего несколько дней назад, с того же видеоустройства, в той же обстановке, при одинаковых уровне и направленности освещения. Согласитесь, в таких условиях добиться высочайшего процента распознавания не так уж и сложно.

Следующая проблема в нашем списке – это видеорегистрация поведения обучающегося во время проведения процедуры тестирования. Увы, в обозримом будущем она так и останется проблемой. Дело не в отсутствии алгоритмов или непроработанности методики. Нет, с этим все в порядке. Причина в технике. Угол обзора камеры, как правило, установленной на мониторе, не позволяет захватить достаточное для качественного контроля пространство вокруг обучающегося. Устранить проблему может только установка камеры в нескольких метрах впереди и минимум 1,5 м выше местонахождения пользователя. Также возможно использование с видеокамерой объектива типа «рыбий глаз» для создания широкоформатного панорамного угла обзора. И тот и другой вариант, увы, технически трудноосуществимы. Поэтому придется довольствоваться тем, что есть. А есть у нас на данный момент пространство, примерно 15-20 см справа, слева и выше обучающегося, и в это пространство, как правило, не попадают руки и предметы, находящиеся на столе. С другой стороны, даже частичный контроль – это во много раз лучше, чем полное отсутствие такового. Остается надеяться, что когда-нибудь решение все же будет найдено.

И, наконец, последняя проблема, точнее, последняя в этой статье.

Если вы помните, выше я писал, что в системе имеется подключение к сети Интернет. Правильнее было бы сказать – к российскому сегменту сети. Что это за подключение – Dial Up, обрывающийся каждые три минуты, GSM, выделенная линия или оптоволоконный канал – мы не знаем. Отсюда вопрос: как передавать видеоряд на сервер в режиме реального времени? Формировать

видео запись на компьютере пользователя и передавать его по окончании тестирования на сервер мы не можем по соображениям безопасности. Транслировать видеоряд напрямую? Увы, нам не известна конфигурация сервера. Скорее всего, это будет не физический сервер, а дисковое пространство на стандартном платном хостинге.

Воротили виртуального мира, такие как Билл Гейтс и прочие АйБиЭмы и эплы вывели особую породу людей – системных администраторов. Главная задача сисадминов – запрещать все, что только возможно, и вообще препятствовать любому проявлению свободомыслия рядовых пользователей. Вы когда-нибудь пробовали уговорить администратора вашего хоста подключить к модулю PHP тысячу раз протестированную на безопасность динамическую библиотеку обработки изображений GDI? И не пытайтесь! Легче о чем угодно договориться с телеграфным столбом. И в какое, извините, место мы должны транслировать наш видеопоток, а главное, как его сохранять?

Мы решили не мудрствовать и принести удобство в угоду простоте и надежности. То есть, вместо формирования видеофильмов и применения новомодных протоколов трансляции видеопотока передавать на сервер ряд последовательных

изображений в формате JPEG, что, кстати, широко распространено для веб-трансляций. Смонтировать в фильм картинки можно будет потом на локальном компьютере. А на крайний случай, с помощью 10 строчек кода java script организовать просмотр в Интернет-браузере. Что мы и сделали. При скорости 1 кадр в секунду за час тестирования наберется 3600 картинок общим объемом около 15-20 Мбт, что вполне приемлемо даже для Dial Up-соединения.

Вряд ли я в своем сумбурном повествовании осветил все принципиально важные аспекты. Скорее всего, вопросов будет больше, чем дано ответов. Тем более что одни только комплексы удаленного контроля не панацея от всех болезней дистанционного образования. Потребуется целый ряд масштабных мероприятий, зачастую весьма далеких от сферы технических средств безопасности. Главное, что первые шаги в этом направлении сделаны.

И в завершение, с разрешения редактора, скажу, что более подробно с аппаратно-программным комплексом удаленного контроля учебного процесса «ВиКонт» можно ознакомиться 24-27 апреля на выставке MIPS-2007 в СК «Олимпийский» на стенде ФГНУ «Главэксперт-центр» и компании «РедТех».

## Техническое регулирование

С 1 июля 2007 года вводится в действие ГОСТ Р 52582-2006 «Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому». Действие стандарта распространяется на механические, электромеханические, электромагнитные замки, замки с электронным управлением (электронные замки с мнемоническим способом введения кода, а также с вещественными носителями кода) и «антипаниковые» замки и устройства, устанавливаемые на защитных конструкциях. Стандарт устанавливает требования к замкам для защитных конструкций по ГОСТ Р 51242, ГОСТ Р 51072, ГОСТ Р 51113, ГОСТ Р 51224, ГОСТ Р 51241, а также методы их испытаний на устойчивость к криминальному открыванию и взлому. В стандарте установлены классы устойчивости замков к криминальному открыванию, требования к их конструкции, к криптостойкости, требования устойчивости к криминальному открыванию, взлому, требования безопасности при проведении испытаний замков.

НОВОСТИ



## Новое имя известного журнала



000 "Все о вашей безопасности"  
 Тел./факс: +7 (495) 631-6467, 631-0036, 688-1536  
 E-mail: total@totalsec.ru www.totalsec.ru