

А.Н. ОРЕШИН, И.Ю. ЛЫСАНОВ  
**НОВЫЙ МЕТОД АВТОМАТИЗАЦИИ ПРОЦЕССОВ  
АУТЕНТИФИКАЦИИ ПЕРСОНАЛА С ИСПОЛЬЗОВАНИЕМ  
ВИДЕОПОТОКА**

---

*Орешин А.Н., Лысанов И.Ю.* **Новый метод автоматизации процессов аутентификации персонала с использованием видеопотока.**

**Аннотация.** На основе проведенных исследований автоматизированных систем управления промышленных предприятий в работе предложена математическая модель аутентификации персонала с использованием технологии формирования и обработки гетерогенного потока, содержащего с источников видеонаблюдения в трафике видеоданных фотографические идентификационные признаки персонала. Отличительной особенностью модели являются операторы переходов и выходов, направленные на формирование сигнала управления по результатам обработки агрегированного потока видеоданных, выделении кадров-вставок, несущих фотографические идентификационные признаки о персонале, сегментации пространства изображения, необходимого для аутентификации персонала в интегрированной системе контроля и управления доступом, а также применение технологий по восстановлению видеопотока. Разработана методика идентификации кадров-вставок в гетерогенном потоке видеоданных, базирующаяся на оценке суммарной дифференциальной экстремальной яркости кадров-сверток, анализе гистограмм изображений кадров по коэффициентам корреляции и полиномам Чебышевской аппроксимации, отличающаяся использованием динамического порога при идентификации кадров и принятия решения об их классе на основе мажоритарного способа обработки данных. Представлены результаты имитационного моделирования процесса аутентификации персонала на основе предложенных модели и методик, позволяющие оценить эффективность визуальной аутентификации персонала при выполнении требований достоверности принятия решения и ограничения пропускной способности сети передачи данных.

**Ключевые слова:** система контроля и управления доступом, система видеонаблюдения, модель, гетерогенный и агрегированный потоки данных, идентификационный признак (биометрический, кодовый и фотографический), кадр-вставка, аутентификация персонала.

---

**1. Введение.** Процедура проверки подлинности чего-либо (аутентификация), включая персонал предприятия, разносторонняя — от оценки введенного пароля или цифровой подписи по открытому ключу проверяемой личности до оценки ее органолептических признаков, биометрических показателей или географического местоположения. При этом нельзя, по-видимому, исключать не только варианты использования расширенной (многофакторной) взаимной аутентификации, сформированной на совместном применении нескольких факторов, но и варианты аутентификации совместно с оценкой возможностей использования субъектом предоставленных ему определенных прав (как сопутствующий процесс авторизации) или совместно с распознаванием субъекта по представленным им идентификационным (то есть совместно с дополнительной идентификацией) [1].

Несмотря на такие возможности аутентификации и обобщенность идеи организации взаимной проверки подлинности, в системах автоматизации промышленных предприятий выделяют компоненты контроля и управления доступом персонала с односторонней аутентификацией, когда только субъект априорно характеризуется некоторой степенью недоверия и требуется подтверждение санкционированного общения (доступа). Как правило, при создании таких подсистем контроля и управления доступом ориентируются на нормативные положения ГОСТ Р ИСО/МЭК [2], ведущая концепция которого, вообще говоря, базируется на двух видах аутентификации — простой, как проверки паролем заявленной идентичности, и строгой, как проверки удостоверения личности.

**2. Актуальность решаемой технической задачи.** В реальности организация санкционированного доступа сводится к разделам ввода идентификационных признаков; отображению оператору видео и фотографических данных субъекта доступа; визуальной идентификации, аутентификации персонала; сбору, хранению и обработке событий. Преимущество централизованного управления и детализация событий на объектах инфраструктуры промышленного предприятия приводят к возрастанию числа точек доступа (ТД), и, как правило, существенному росту интенсивности их использования при потребности соответствующего сокращения времени на аутентификацию персонала. В условиях ограниченного времени эти факторы принципиально сужают возможности оператора по исполнению функций с требуемыми показателями качества.

Известные разработки систем контроля и управления доступом [3, 4, 5] ведущих производителей PERCo (РФ), Parsec (РФ), Gate (РФ), Anviz Biometric Inc (США), APOLLO (США), Honeywell (США), Bosch Security Systems (Германия) и SYNEL (Израиль) не позволяют обеспечить решение вопросов визуальной аутентификации персонала оператором уже при количестве точек доступа, большим 8-12. Результаты исследований PSDB (Великобритания) показали, что восприятие человеком изображения на мониторах ухудшается с увеличением их количества (с 85% для одного, до 53% для девяти).

Кроме того, известный методический материал отечественных и зарубежных ученых В.А. Ворона, Р.Г. Магауенова, В.А. Тихонова, Г. Кругля, М. Гарсиа, В. Дамьяновски [4, 7] не касается вопросов централизованного контроля и управления доступом по результатам идентификации и аутентификации персонала с фотографических данных, а в большей степени затрагивает структуру системы видеонаблюдения совместно с техническими (реакция на код, электронный ключ, пластиковая карта, радиочастотная метка и т. п.) или биометрически-

ми (считыватель отпечатков пальцев, рисунка сетчатки глаза, геометрии ладони и лица и т. п.) идентификаторами на локальных участках точек доступа [7-10].

С другой стороны, применение систем видеонаблюдения позволяет оператору осуществлять контроль территориально удаленных объектов инфраструктуры, но не дает детального представления об их состояниях, о санкционированном пребывании и численности персонала в интересующей среде обитания в реальном масштабе времени. Причем влияние «человеческого фактора» (эмоциональная напряженность, снижение внимания, случайное отвлечение, несанкционированное прерывание деятельности) существенно уменьшает адекватность и оперативность принятия решений.

Каждый из представленных подходов (идентификация по фото или видео) анализирует ограниченный набор идентификационных признаков под определенным углом зрения. Совместное (гибридное) их использование генерирует новый источник информации, характеризующийся многофакторной оценкой идентификационных признаков, необходимый для аутентификации персонала. Поэтому разработка метода аутентификации персонала, используя видеопоток для передачи идентификационных признаков (в частности фотографических), не только актуальна, но и научно необходима и технически целесообразна.

**3. Математическая модель аутентификации персонала в интегрированной системе контроля и управления доступом.** Представим математическую модель [11] аутентификации персонала в виде множества (1):

$$Q_{СКВД} = \{T, S_{ПД}(t), X_{ПД}(t), Y_{ПД}(t), K_{ВП}(t), K_{ПКВ}(t), K_{ГП}(t), Q_{СПД}, Q_{ЦПП}, F_1, F_2, F_3, F_4\}, \quad (1)$$

элементами которого являются подмножества, характеризующие в момент времени  $t \in T$ : состояния пространства доступа (ПД)  $S_{ПД}(t)$ ; входные воздействия на пространства доступа  $X_{ПД}(t)$ ; реакции пространства доступа  $Y_{ПД}(t)$ ; видеопоток  $K_{ВП}(t)$ ; поток кадров-вставок  $K_{ПКВ}(t)$ ; гетерогенный поток  $K_{ГП}(t)$ , а также подмножества, описывающие структуру сети передачи данных  $Q_{СПД}$  [12] и цветовое пространство пикселя  $Q_{ЦПП}$  модели *RGB* [13, 14]; механизм изменения состояний пространства доступа по входным воздействиям ( $F_1$ ) и формирования выходного сигнала как реакцию пространства доступа на внутренние и внешние воздействия ( $F_2$ ), а также

операторы формирования гетерогенного потока ( $F_3$ ) и выделения кадров-вставок и восстановления видеопотока ( $F_4$ ).

$$F_1: T \times X_{ПД}(t) \times S_{ПД} \rightarrow S_{ПД}; \quad (2)$$

$$F_2: T \times X_{ПД}(t) \times S_{ПД} \rightarrow Y_{ПД}; \quad (3)$$

$$F_3: K_{ВП}(t), K_{ПКВ}(t) \rightarrow K_{ГП}(t) = K_{ВП}(t) \cup K_{ПКВ}(t); \quad (4)$$

$$F_4: K_{ГП}(t) \rightarrow K_{ВП}(t), K_{ПКВ}(t). \quad (5)$$

Требуется реализовать операторы формирования гетерогенного потока ( $F_3$ ), а также выделения кадров-вставок  $K_{вст_k} \in K_{ПКВ}(t) = K_{вст_1}, K_{вст_2}, \dots, K_{вст_k}, \dots$  и восстановления видеопотока  $K_{ВП}(t) = K_{вид_1}, K_{вид_2}, \dots, K_{вид_k}, \dots$  ( $F_4$ ), обеспечивающие автоматизацию процесса аутентификации персонала и управления доступом на максимальном количестве точек доступа (ТД):

$$\sum_{m=1}^{N^{3Д}} \sum_{n=1}^{N^{ТД}} N_{m,n}^{ТД} \Rightarrow \max, \quad (6)$$

где  $N^{3Д}$  — количество зон доступа в пространстве доступа;  $N^{ТД}$  — количество точек доступа в  $n$ -ой зоне доступа;  $N_{m,n}^{ТД}$  — точка доступа в  $m$ -ом пространстве доступа,  $n$ -ой зоны доступа, при ограничениях:

$$\forall K_{ГП}^n(t) \in K_{ГП}^{ПД}(t) \Rightarrow K_{ГП}^n = K_{ВП}^n, \quad (7)$$

$$\forall K_{ГП}^n(t) \in K_{ГП}^{ПД}(t) \Rightarrow K_{ПКВ}^n \leq 3, \quad (8)$$

$$Q_{СПД} = \text{const}, q_{СМО} \geq q_{СМО}^{mp}, \quad (9)$$

где  $K_{ГП}^n$  — число кадров в одну секунду в гетерогенном потоке;  $K_{ВП}^n$  — число кадров в одну секунду в видеопотоке;  $K_{ПКВ}^n$  — число подряд идущих в гетерогенном потоке кадров-вставок;  $Q_{СПД}$  — структура сети передачи данных [15];  $q_{СМО}$  — относительная пропускная способность системы контроля и управления доступом с визуальной аутентификацией персонала, рассматриваемой как система массового

обслуживания [16];  $K_{ГП}^{ПД}(t)$  — множество гетерогенных потоков в пространстве доступа.

Данная модель базируется на технологии формирования и обработки гетерогенного потока  $K_{ГП}(t) = K_{пот1}, K_{пот2}, \dots, K_{потk}, \dots = K_{ВП}(t) \cup K_{ПКВ}(t)$ , содержащего видеокадры  $K_{видk'} \in K_{ВП}(t) = K_{вид1}, K_{вид2}, \dots, K_{видk'}, \dots$  и кадры-вставки  $K_{вст} \in K_{ПКВ}(t) = K_{вст1}, K_{вст2}, \dots, K_{встk'}, \dots$

Математическая модель основывается на передаче кадров-вставок (растровых изображений), несущих фотографические данные о субъекте доступа, при котором  $k$ -ый кадр гетерогенного потока представляется в виде множества пикселей  $\pi_{i,j}^k$  на плоскости изображения и математически описывается матрицей  $\kappa_{nomk} = \left\| \pi_{i,j}^k \right\|, i = \overline{1, I}, j = \overline{1, J}$ , где  $k$  — номер кадра,  $i$  и  $j$  — номера столбца и строки матрицы [17, 18, 19]. Изображение кадра гетерогенного потока представим в виде множества цветowych точек  $c_{i,j}^k$ , соответствующих каждому пикселю  $\pi_{i,j}^k$  модели  $RGB$ :  $I_k = \left\| c_{i,j}^k \right\|, i = \overline{1, I}, j = \overline{1, J}$ .

В модели аутентификации персонала введены следующие обозначения (рисунок 1):

- К — контроллер;
- БФПВК — блок формирования потока видеокладов;
- БФПКВ — блок формирования потока кадров-вставок;
- БФГП — блок формирования гетерогенного потока;
- ОД — объект доступа;
- БАОД — блок аутентификации объектов доступа;
- БИКВ — блок идентификации кадров-вставок;
- БИОДБП — блок идентификации ОД по биометрическому

признаку;

- БИОДКП — блок идентификации ОД по кодовому признаку;
- входные воздействия на точки доступа (ТД)

$\vec{x} = (x_{УПУ}, x_{ГБР}, x_{БУ})$ ,  $\vec{x} \in X(t)$ , элементами которого являются воздействия на управляемое преграждающее устройство (УПУ)  $x_{УПУ}$ , группу быстрого реагирования (ГБР)  $x_{ГБР}$  и блокирующее устройство (БУ)  $x_{БУ}$ ;

– реакция точки доступа  $\vec{y} = (y_{ОД}, y_{УПУ}, y_{ГБР}, y_{БУ}, y_{СС})$ ,  $\vec{y} \in Y(t)$ , элементами которого являются величины характеризующие состояния ОД  $s_{ОД}$ , УПУ  $s_{УПУ}$ , ГБР  $s_{ГБР}$ , БУ  $s_{БУ}$  и системы сигнализации (СС)  $s_{СС}$ .

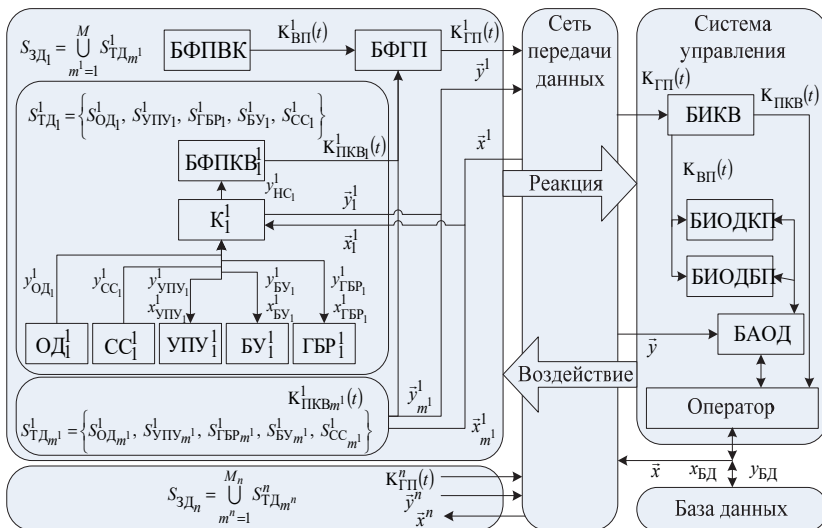


Рис. 1. Модель аутентификации персонала в интегрированной системе контроля и управления доступом

При этом состояние точки доступа  $\vec{s}_{ТД} = (s_{ОД}, s_{УПУ}, s_{ГБР}, s_{БУ}, s_{СС}) \in S_{ТД}$  характеризуется в произвольный момент времени  $t \in T$  набором переменных, изменяющихся под влиянием воздействий  $\vec{x}$ , формируемых контроллером. Состояние зоны доступа  $S_{зД}$  определяется входящими в нее ТД. Взаимодействие с базой данных (БД) определяется воздействиями  $x_{БД}$  и реакцией  $y_{БД}$ .

Множество состояний ТД описывается выражением  $S_{ТД} = \{S_{ОД}, S_{УПУ}, S_{ГБР}, S_{БУ}, S_{СС}\}$ , где:

–  $S_{ОД} = \{S_{НОД}, S_{КП}, S_{БП}\}$  — множество состояний объекта доступа;

- $S_{\text{НОД}} = \{S_{\text{НОД}_1}, S_{\text{НОД}_2}\}$  — множество состояний ОД по его нахождению в ТД;
- $S_{\text{БП}} = \{S_{\text{БП}_1}, S_{\text{БП}_2}\}$  — множество состояний ОД по наличию у него биометрического признака;
- $S_{\text{КП}} = \{S_{\text{КП}_1}, S_{\text{КП}_2}\}$  — множество состояний объекта доступа по наличию у него кодового идентификатора;
- $S_{\text{БУ}} = \{S_{\text{БУ}_1}, S_{\text{БУ}_2}\}$  — множество состояний блокирующих устройств;
- $S_{\text{СС}} = \{S_{\text{ДСС}_i}\}$  — множество состояний системы сигнализации, характеризующееся состояниями датчиков;
- $S_{\text{УПУ}} = \{S_{\text{УПУ}_1}, S_{\text{УПУ}_2}\}$  — множество состояний УПУ;
- $S_{\text{ГБР}} = \{S_{\text{ГБР}_1}, S_{\text{ГБР}_2}\}$  — множество состояний ГБР;

Реакция на нестандартное событие  $y_{\text{НС}}$  формируется в случаях, когда:

- идентификационный признак не соответствует субъекту доступа (отказ в допуске);
- необходимо осуществить допуск в ручном режиме;
- время пребывания субъекта доступа в ТД выходит за рамки установленного;
- аварии на линии между контролером и сервером или влияние на нее злоумышленника с целью скрытия реального события на ТД (при наличии связи между сервером и контроллером события автоматически транслируются на сервер системы контроля и управления доступом персонала [3, 4, 5]);
- срабатывают датчики систем сигнализации (пожарной, тревожной, охранной и т. д.).

Предложенная математическая модель автоматизации процессов аутентификации персонала позволяет определить стратегию развития систем контроля и управления доступом (СКУД) на основе технологии формирования и обработки гетерогенного потока при выполнении требований достоверности и адекватности принятия решения, а также ограничении пропускной способности сети передачи данных.

**4. Методика идентификации кадров-вставок в гетерогенном потоке видеоданных, сегментации пространства изображения и восстановления видеопотока.** В алгоритмическом виде методика представлена на рисунке 2.

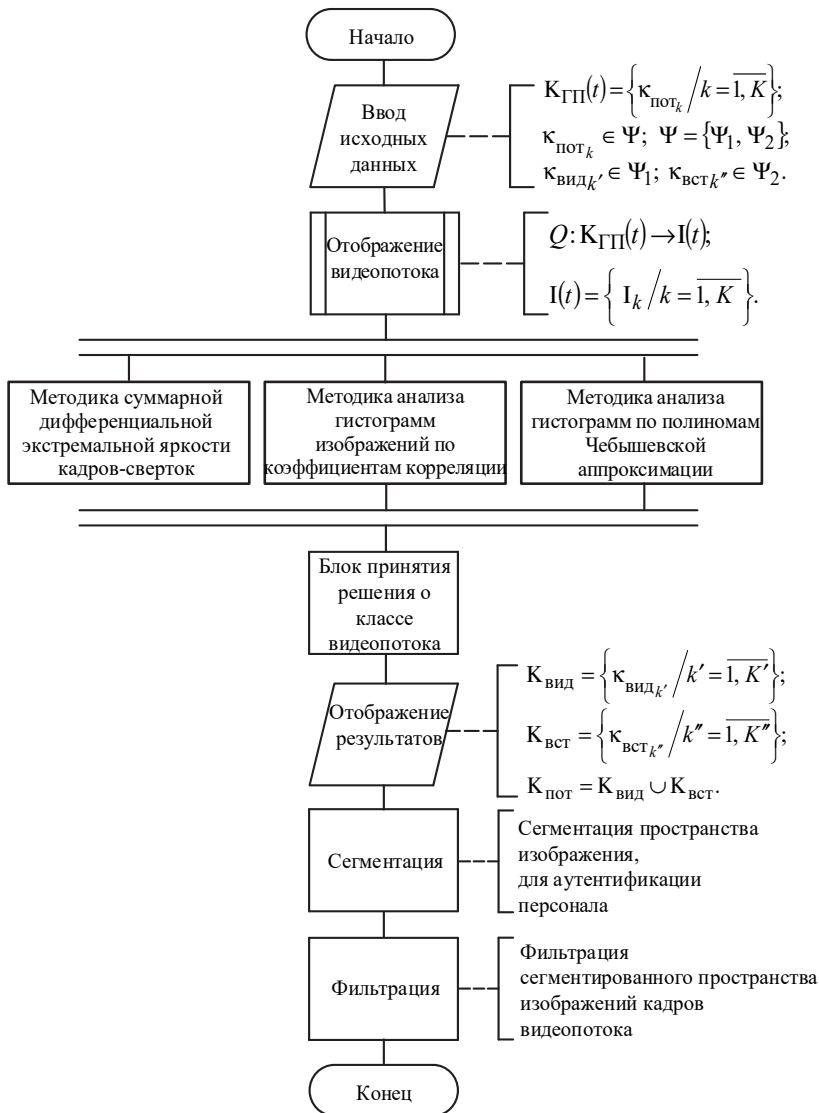


Рис. 2. Алгоритм идентификации кадров-вставок в гетерогенном потоке видеоданных, сегментации пространства изображения и восстановления видеопотока

Суть методики состоит в следующем:



1. На первом этапе осуществляется ввод гетерогенного потока видеоданных  $K_{ГП}(t) = \kappa_{пот1}, \kappa_{пот2}, \dots, \kappa_{потk}, \dots$  — множество кадров в потоке видеоданных [20];

$\Psi_1, \Psi_2 \in \Psi$  — множество классов кадров в гетерогенном потоке;

$\Psi_1$  — класс кадров видеопотока  $\kappa_{видk'} \in \Psi_1$ ;

$\Psi_2$  — класс кадров-вставок  $\kappa_{встk''} \in \Psi_2$ , несущих фотографические данные о персонале.

2. Второй этап заключается в отображении кадра гетерогенного потока в растровое изображение  $Q: K_{ГП}(t) \rightarrow I(t)$ , где

$$I(t) = \left\{ I_k / k = \overline{1, K} \right\}.$$

3. На третьем этапе формируется наблюдаемое окно  $I_{окн} = \left\{ I_k / k = \overline{1, 8} \right\}$ .

4. Четвертый этап сводится к идентификации кадра-вставки тремя подходами с разными порогами чувствительности на основе:

*Оценки суммарной дифференциальной экстремальной яркости кадров-сверток (попиксельной разности изображений кадров гетерогенного потока) [21-23].*

Оценка класса кадра  $\Psi_1, \Psi_2 \in \Psi$  (рисунок 3) осуществляется способом сравнения экстремальной яркостной составляющей кадра-свертки  $C_{k,k+1} \in C_{сверт}$  [13], где  $k = \overline{4, 7}$  с динамически изменяющимся пороговым значением  $C_{пор1}$  (10):

$$C_{пор1} = \frac{\sum_{k=1}^3 C_{k,k+1}}{3} + \Delta_1, \quad (10)$$

где  $\Delta_1$  — абсолютная погрешность экстремальной яркостной составляющей, определяемая по результатам статистических данных о видеопотоке;  $C_{k,k+1} \in C_{сверт}$  — попиксельная разность по  $r_{ij}^k, g_{ij}^k, b_{ij}^k$  составляющим цвета  $c_{ij}^k$  пикселя  $\pi_{i,j}^k$  модели *RGB*:

$$C_{k,k+1} = \sum_{i=1}^I \sum_{j=1}^J \left| r_{i,j}^k - r_{i,j}^{k+1} \right| + \sum_{i=1}^I \sum_{j=1}^J \left| g_{i,j}^k - g_{i,j}^{k+1} \right| + \sum_{i=1}^I \sum_{j=1}^J \left| b_{i,j}^k - b_{i,j}^{k+1} \right|. \quad (11)$$

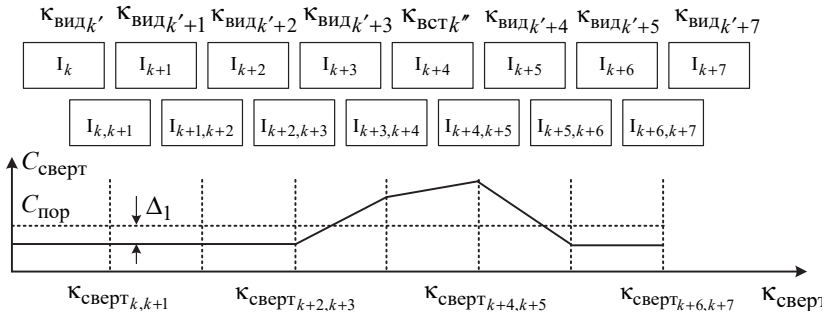


Рис. 3. Оценка суммарной дифференциальной экстремальной яркости изображений кадров-сверток

В случае, когда вторая граница  $C_{k,k+1} \in C_{\text{сверт}}$ , превышающая  $C_{\text{пор}}$ , выходит за границы исследуемого окна — регистрируется следующий сюжет, то есть  $K_{\text{пот}k'} \in \Psi_1$ .

Анализа гистограмм изображений кадров по коэффициентам корреляции [24].

Для анализа изображений кадров  $K_{\text{пот}k}$  исследуемого окна используется закон распределения  $p^k(\xi)$  величин  $r_{ij}^k$ ,  $g_{ij}^k$ ,  $b_{ij}^k$  цвета  $c_{ij}^k$  пикселя  $\pi_{i,j}^k$ , устанавливающий связь между значениями интенсивностями  $\xi_{i,\varepsilon}^k$  цветов пикселя  $k$ -ого кадра и соответствующими им статистическими вероятностями  $p^k(\xi_{i,\varepsilon}^k)$ .

Решения о классе кадра  $\Psi_1, \Psi_2 \in \Psi$  (рисунок 4) принимается по результатам сравнения оценок коэффициентов корреляции кадров декодированного гетерогенного потока видеоданных  $\tilde{K}_{k,k+1}(\xi)$  со средними значениями оценок коэффициентов корреляции  $\tilde{K}_{\text{средн}k}(\xi)$  [20, 24] по критерию (12):

$$\tilde{K}_{\text{средн}k+h}(\xi) > \tilde{K}_{k+h,k+h+1}(\xi) + \Delta_2, h = \overline{0,6}, \quad (12)$$

где:

$$\tilde{K}_{k,k+1}(\xi) = \frac{\sum_{i^\varepsilon=1}^{256} \left( \xi_{i^\varepsilon}^k - \tilde{m}_{p^k(\xi)} \right) \left( \xi_{i^\varepsilon}^{k+1} - \tilde{m}_{p^{k+1}(\xi)} \right)}{255 \times \tilde{\sigma}_{p^k(\xi)} \tilde{\sigma}_{p^{k+1}(\xi)}}, \quad (13)$$

$$\tilde{K}_{\text{средн}_k}(\xi) = \frac{\tilde{K}_{k,k+1}(\xi) + \tilde{K}_{k+1,k+2}(\xi) + \tilde{K}_{k,k+3}(\xi)}{3}, \quad (14)$$

оценки математического ожидания интенсивности изображения кадра и среднеквадратичного отклонения:

$$\tilde{m}_{p^k(\xi)} = \sum_{i^\xi=1}^{256} p^k(\xi_{i^\xi}^k) \times \xi_{i^\xi}^k, \quad (15)$$

$$\tilde{\sigma}_{p^k(\xi)} = \sqrt{\tilde{D}_{p^k(\xi)}} = \sqrt{\frac{\sum_{i^\xi=1}^{256} \left( \xi_{i^\xi}^k - \tilde{m}_{p^k(\xi)} \right)^2}{255}}, \quad (16)$$

$\Delta_2$  — абсолютная погрешность, определяемая эмпирически.

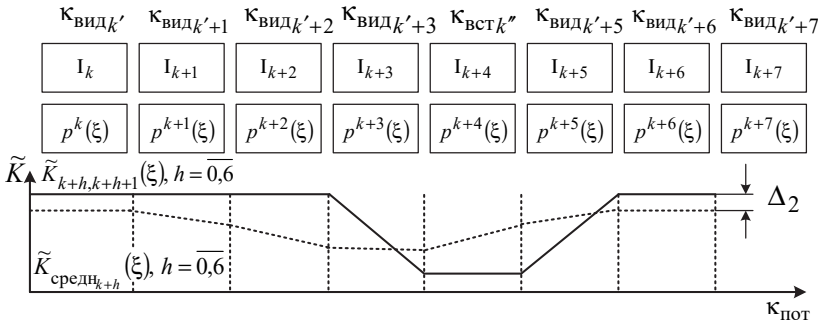


Рис. 4. Анализ гистограмм изображений кадров по коэффициентам корреляции

*Анализа гистограмм изображений кадров по полиномам Чебышевской аппроксимации [20, 25].*

Принимается решение о классе кадров входного потока (рисунок 5) по результатам поэлементного сравнения варьируемых параметров  $A_n$  и  $B_m$  дробей Чебышева  $f(\xi)$  всех 24 гистограмм

$p^{k^o}(\xi)$ ,  $k^o = \overline{1,8}$ ,  $\xi \in (r, g, b)$ , множеств разностей матриц

$H_{k+h,k+h+1}$ ,  $h = \overline{3,6}$  в наблюдаемом окне с пороговым значением (17):

$$\sup \left\{ H_{k+h,k+h+1} / h = \overline{0,2} \right\} + \Delta_3, \quad (17)$$

где:

$$f(\xi) = \frac{A_0 \xi^N + A_1 \xi^{N-1} + \dots + A_N}{\xi^M + B_1 \xi^{M-1} + \dots + B_M}, \quad (18)$$

$A_n, n = \overline{1, N}$  — параметры числителя дроби, а  $B_m, m = \overline{1, M}$  — параметры знаменателя дроби,

$$\mathbf{H}_{k,k+1} = \left| \mathbf{H}_k - \mathbf{H}_{k+1} \right| = \begin{vmatrix} A_{n_0}^{k,k+1} & A_{n_1}^{k,k+1} & \dots & A_{n_N}^{k,k+1} & B_{n_0}^{k,k+1} & B_{n_1}^{k,k+1} & \dots & B_{n_M}^{k,k+1} \\ A_{g_0}^{k,k+1} & A_{g_1}^{k,k+1} & \dots & A_{g_N}^{k,k+1} & B_{g_0}^{k,k+1} & B_{g_1}^{k,k+1} & \dots & B_{g_M}^{k,k+1} \\ A_{b_0}^{k,k+1} & A_{b_1}^{k,k+1} & \dots & A_{b_N}^{k,k+1} & B_{b_0}^{k,k+1} & B_{b_1}^{k,k+1} & \dots & B_{b_M}^{k,k+1} \end{vmatrix}, \quad (19)$$

$\Delta_3$  — абсолютная погрешность, определяемая по результатам экспериментов.

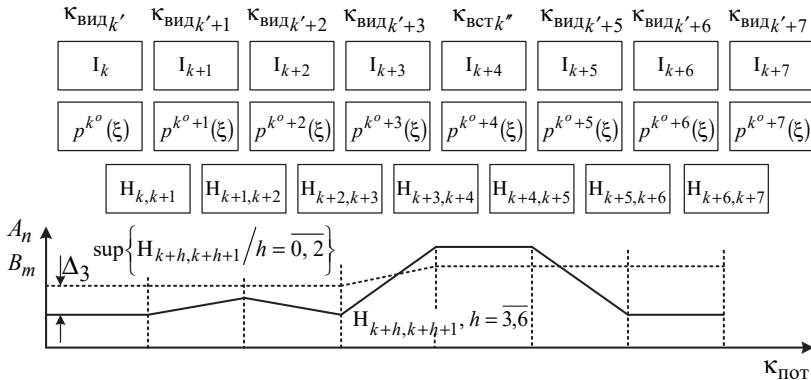


Рис. 5. Анализ гистограмм изображений кадров по полиномам Чебышевской аппроксимации

5. На пятом этапе принимается решения о классе кадров гетерогенного потока по мажоритарному правилу [20]. Параллельное применение представленных методик позволяет идентифицировать кадры-вставки, несущие фотографические данные о персонале, при следующих ограничениях:

- число кадров в визуальной вставке меньше трех;
- стартовые четыре кадра наблюдаемого окна не являются вставкой;

- кадр-вставка не граничит с разными сюжетными линиями.

6. На шестом этапе осуществляется сегментация пространства изображения, идентифицированного кадра-вставки, необходимого для аутентификации персонала. Математическое обоснование способов сегментации пространства изображения заключается в определении производных, представленных в виде дискретных приближений градиента для цифровых изображений [26]. В качестве градиентных способов выделяют операторы Собеля, Робертса, Гаусса, Лапласиана, Преветта и другие [21, 27, 28].

7. Заключительный этап направлен на восстановление и отображение видеопотока. Для фильтрации сегментированного пространства с идентифицированных кадров воспользуемся технологией «Морфинг» [29]. В качестве основы функционирования данного процесса определяются контрольные точки. Вокруг данных точек и происходит плавная трансформация одного набора пикселей в другой путем их корректной замены.

**5. Моделирование и экспериментальное исследование процессов формирования и обработки гетерогенного потока с фотографическими данными о персонале.** Для оценки эффективности визуальной аутентификации персонала разработана имитационная модель, представленная на рисунке 6.

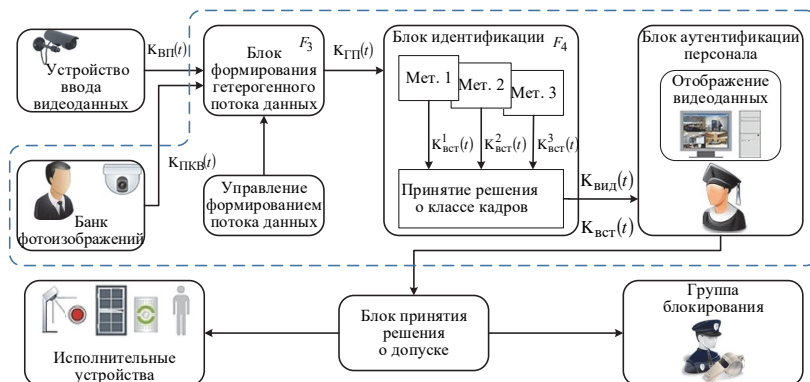


Рис. 6. Структура имитационной модели формирования гетерогенного потока видеоданных и идентификации кадров-вставок

Основными элементами имитационной модели являются:

- поток видеок кадров, поступающий с устройства ввода видеоданных  $K_{ВП}(t) = \kappa_{вид1}, \kappa_{вид2}, \dots, \kappa_{видk'}, \dots;$
- банк фотоизображений, используемый для формирования потока кадров-вставок, несущих фотографические данные о персонале  $K_{ПКВ}(t) = \kappa_{вст1}, \kappa_{вст2}, \dots, \kappa_{встk'}, \dots;$
- блок формирования гетерогенного потока  $K_{ГП}(t)$ , содержащего видеок кадры  $\kappa_{видk'} \in \Psi_1$  и кадры-вставки  $\kappa_{встk'} \in \Psi_2;$
- блок управления агрегированным потоком данных, определяющий структуру гетерогенного потока;
- блок, реализующий методику идентификации кадров-вставок в гетерогенном потоке видеоданных, сегментации пространства изображения и восстановления видеопотока;
- блок вывода результатов, отображающий на мониторе ЭВМ отдельно множество видеок кадров и множество кадров-вставок.

Имитационная модель реализована с использованием среды графического программирования LabVIEW [13, 19], языка программирования C++ и библиотеки компьютерного зрения OpenCV.

Имитируя с помощью ЭВМ процессы формирования гетерогенного потока и идентификации кадров-вставок четырьмя алгоритмами (рисунок 6) как в отдельности, так и в совокупности, получим оценки характеристик разработанного метода, представленные в таблице 1.

Таблица 1. Результаты экспериментального исследования алгоритмов идентификации кадров-вставок в гетерогенном потоке

Метод идентификации	Частота пропуска кадра-вставки	Частота ложного обнаружения кадравставки
Суммарной дифференциальной яркости (существующий)	0,21	0,54
Суммарной дифференциальной экстремальной яркости кадров-сверток с динамическим порогом	0,20	0,12
Анализа гистограмм изображений кадров по коэффициентам корреляции	0,34	0,18
Анализа гистограмм изображений кадров по полиномам Чебышевской аппроксимации	0,27	0,13
Алгоритм аналитической обработки выделенных кадров	0,13	0,07

Учитывая различные пороги чувствительности представленных подходов к цветовым характеристикам изображений кадров видеопотока, наименьшие частоты пропуска или ложного обнаружения кадров-вставок соответствуют разработанному новому методу с параллельным применением трех методик и дальнейшей аналитической обработкой выделенных кадров.

Для оценки эффективности функционирования интегрированной СКУД процесс визуальной аутентификации персонала оператором опишем системой массового обслуживания (СМО), где  $\lambda_{СМО}$  — интенсивность входящего потока кадров-вставок на обслуживание;  $\mu_{СМО}$  — интенсивность выходящего потока обслуженных кадров-вставок;  $\rho_{СМО} = \lambda_{СМО} / \mu_{СМО}$  — приведенная интенсивность потока кадров-вставок;  $q_{СМО}$  — относительная пропускная способность СМО (показатель эффективности функционирования).

Существующие в настоящее время СКУД с визуальной аутентификацией персонала можно рассматривать как СМО с отказами, при этом число каналов обслуживания  $n_{СМО}$  равно количеству операторов.

Разработанный метод представляет новую концепцию визуальной аутентификации персонала в СКУД, изменив дисциплину обслуживания заявок (несущих фотографические данные о СД) с отказами на СМО с комбинированным способом обслуживания (ограничение по длине очереди), где  $m_{СМО}$  — длина очереди.

Зависимости  $q_{СМО}$  от  $\rho_{СМО}$ , отраженные на рисунке 7, свидетельствуют о повышении эффективности визуальной аутентификации персонала в интегрированной системе контроля и управления доступом.

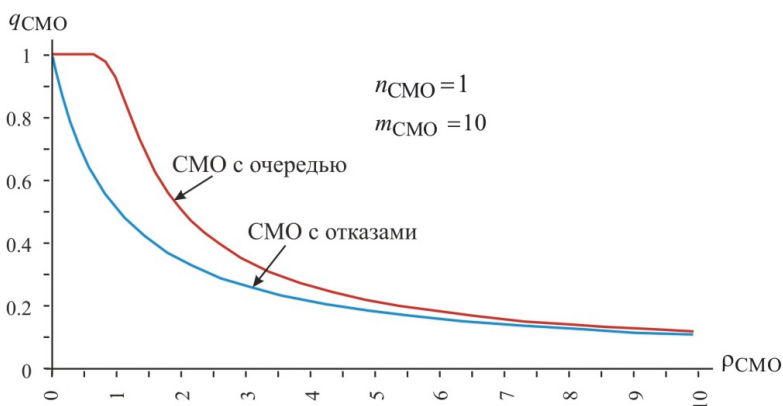


Рис. 7. Зависимость  $q_{СМО} = \phi_1(\rho_{СМО}, m_{СМО})$ , при  $m_{СМО} = 10$

Кроме того, если оператор наблюдает за несколькими мониторами одновременно, точность визуальной аутентификации уменьшается и составляет: 85% при одном, 74% — четырех, 58% — шести и 53% при девяти мониторах. При обслуживании заявок, поступающих из очереди, оператору необходимо наблюдать всего за одним монитором, таким образом, при увеличении количества ТД вероятность правильного принятия решения остается постоянной величиной.

Формирование гетерогенного потока видеоданных для передачи статических изображений несущих информацию о персонале позволяет увеличить количество ТД при заданной пропускной способности сети передачи данных. Зависимость количества точек доступа от интенсивности появления персонала в ТД показана на рисунке 8.

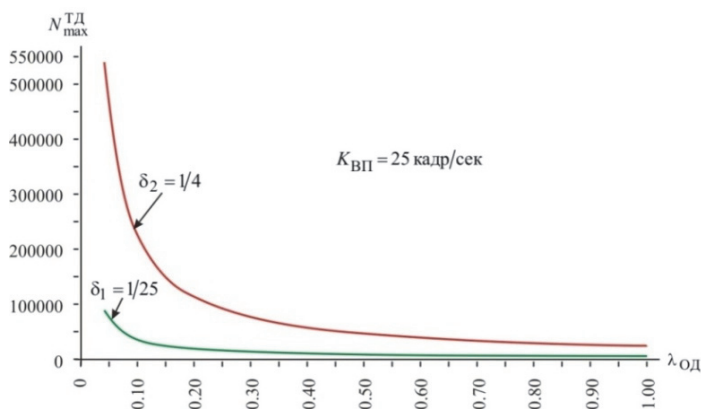


Рис. 8. Зависимость  $N_{\max}^{\text{ТД}} = \phi_2(\tilde{\lambda}_{\text{ОД}}, \delta)$ , при  $K_{\text{ВП}} = 25$  кадр/сек

В данных зависимостях были использованы следующие обозначения:  $N_{\max}^{\text{ТД}}$  — потенциальные возможности зоны доступа (максимальное количество точек доступа);  $K_{\text{ВП}}$  — кадровая частота видеопотока (количество кадров в единицу времени в видеопотоке), входящего в гетерогенный поток;  $\tilde{\lambda}_{\text{ОД}} = \frac{1}{N^{\text{ТД}}} \sum_{m=1}^{N^{\text{ТД}}} \tilde{\lambda}_{\text{ОД}_m}$  — средняя интенсивность появления персонала в точках доступа анализируемой зоны доступа;  $\delta = K_{\text{ПВК}}/K_{\text{МП}}$  — относительное значение количества кадров-вставок к числу кадров гетерогенного потока.

Поскольку имитационная модель описывает процесс функционирования проектируемой интегрированной СКУД, которая в данный



момент не существует, проверка адекватности в классическом понимании не реализуема. В работе проверка адекватности осуществлялась путем проведения натурального эксперимента. Гетерогенный поток видеоданных сформирован на основе реальных устройств системы видеонаблюдения. Проанализировано 45 реализаций, включающих 270 тысяч кадров, из которых 5,5 тысяч кадров-вставок.

**6. Заключение.** По результатам анализа известных технологий аутентификации персонала разработана математическая модель, использующая кадр-вставку для передачи статических изображений, базирующаяся на технологии формирования и обработки гетерогенного потока видеоданных, характеризующаяся структурой сети передачи данных, механизмом изменения состояний точек доступа по входным воздействиям и их реакции на внутренние и внешние воздействия, позволяющая значительно увеличить количество наблюдаемых объектов при заданных вероятности правильного принятия решения и пропускной способности сети передачи данных.

Разработана методика идентификации кадров-вставок в потоке видеоданных, базирующаяся на оценке суммарной дифференциальной экстремальной яркости кадров-сверток, анализе гистограмм изображений кадров по коэффициентам корреляции и полиномам Чебышевской аппроксимации, отличающаяся использованием динамического порога при идентификации кадров и принятия решения об их классе на основе мажоритарного способа обработки данных.

Разработана имитационная модель процесса формирования гетерогенного потока и идентификации кадров-вставок на основе предложенной математической модели и методики, позволяющая провести ее верификацию и валидацию на предмет подтверждения адекватности применения теоретических положений. Частоты пропуска и ложного обнаружения кадров-вставок уменьшились минимум в 1,5 раза. Эффективность визуальной аутентификации персонала в интегрированной СКУД в диапазоне от 0,1 до 10 приведенной интенсивности потока кадров-вставок, несущих фотографические данные о персонале, повышена не менее чем на 10%.

Представлен новый метод аутентификации персонала, позволяющий передавать через видеопоток идентификационные признаки субъекта доступа, необходимые для одновременного отображения реальных и эталонных фотографических данных в интегрированных СКУД на промышленных предприятиях.

## Литература

1. *Козачок А.В., Бочков М.В., Фаткиева Р.Р., Туан Л.М.* Аналитическая модель защиты файлов документальных форматов от несанкционированного доступа // Труды СПИИРАН. 2015. Вып. 6(43). С. 228–252.
2. ГОСТ Р ИСО/МЭК 9594-8-98 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации // М.: Госстандарт России. 1998.
3. *Novak T., Gerstinger A.* Safety and Security-Critical Services in Building Automation and Control Systems // *Industrial Electronics. IEEE.* 2010. vol. 57. pp. 3614–3621.
4. Официальный сайт компании PERCo. URL: [www.perco.ru](http://www.perco.ru) (дата обращения: 17.08.2015).
5. Официальный сайт компании Anviz Biometric Inc. URL: [www.anviz.com](http://www.anviz.com) (дата обращения: 6.05.2015).
6. *Ibrahim R., Zin Z.* Study of automated face recognition system for office door access control application // *IEEE 3rd International Conference on Communication Software and Networks (ICCSN).* 2011. pp. 132–136.
7. *Лалина Т.И., Енушеев Н.Н., Лалин Д.В.* Способ биометрической аутентификации пользователя в компьютеризованных системах контроля доступа // Труды СПИИРАН. 2013. Вып. 4(27). С. 189–199.
8. *Park J., Lin S.* A random effect model for reconstruction of spatial chromatin structure // *Biometrics journal of the International Biometric Society.* 2017. vol. 73. no. 1. pp. 52–62.
9. *Shen C. et al.* Identification of subpopulations with distinct treatment benefit rate using the Bayesian tree // *Biometrical Journal.* 2016. vol. 58. no. 6. pp. 1357–1375.
10. *Бутрина А.В., Бугаева А.П.* Биометрическая идентификация личности // Актуальные проблемы авиации и космонавтики. 2012. № 8. С. 389–390.
11. *Цеханоский В.В., Чертовской В.Д.* Математическая модель многоуровневой адаптивной автоматизированной системы управления производством // Вестник Нижневартского государственного университета. 2014. № 3. С. 86–95.
12. *Орешин А.Н., Орешин Н.А., Шумилин В.С., Панчук П.В.* Методика оптимального распределения каналов и трактов на основе определения продуктивных путей с помощью автоматизированных систем управления связью // Телекоммуникации. 2016. № 10. С. 44–48.
13. *Визильтер Ю. и др.* Обработка и анализ цифровых изображений с примерами на LabVIEW и IMAQ Vision // М.: ДМК Пресс. 2008. 464 с.
14. *Харинов М.В.* Модель цифрового изображения с виртуальной памятью на основе псевдотройной системы счисления // Труды СПИИРАН. 2007. Вып. 4. С. 126–135.
15. *Трегубов Р.Б., Алексиков Ю.Г., Саитов С.И.* Представление иерархических много-уровневых маршрутизирующих систем в теоретико-множественном базисе // Труды СПИИРАН. 2016. № 1(44). С. 139–168.
16. *Трегубов Р.Б., Саитов И.А.* Теоретические основы анализа и оптимизации иерархических многоуровневых маршрутизирующих систем // Орел: Академия ФСО России. 2017. 585 с.
17. *Сальников И.И., Мартенс-Атюшев Д.С.* Методы цифровой обработки изображений // Международный студенческий научный вестник. 2015. № 3-2. С. 276–277. URL: [www.eduherald.ru/article/view?id=12478](http://www.eduherald.ru/article/view?id=12478) (дата обращения: 04.03.2017).
18. *Гонсалес Р., Вудс Р., Чоуи П.А.* Мир цифровой обработки. Цифровая обработка изображений // М.: Техносфера. 2006. 1072 с.
19. *Shapiro L., Stockman G.C.* Computer Vision // New Jersey. Prentice-Hall. 2001. pp. 279–325.

20. *Орешин А.Н., Саитов И.А., Орешин Н.А.* Стратегия повышения качества услуг видеосвязи на основе фильтрации видеопотока, содержащего кадры-вставки с информационным шумом // Труды СПИИРАН. 2015. № 4(41). С. 57–81.
21. *Харинов М.В., Ханьков И.Г.* Комбинированный метод улучшения сегментации изображения // Вестник Бурятского государственного университета. Серия. Математика и информатика. 2015. Вып. 9. С. 118–124.
22. *Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К.* Алгоритмы: построение и анализ. 3-е издание // М.: Издательский дом "Вильямс". 2013. 1323 с.
23. *Орешин А.Н., Скурнович А.В., Кирухин Д.А.* Способ идентификации кадров-вставок в потоке мультимедийных данных. Патент на изобретение № 2506640. 2014.
24. *Орешин А.Н., Лысанов И.Ю.* Методика идентификации кадра-вставки в потоке видеоданных на основе корреляционного анализа гистограмм изображений кадров с динамическим порогом принятия решения // Информационные системы и технологии. 2014. № 6. С. 129–138.
25. *Лысанов И.Ю., Орешин А.Н.* Идентификация кадра-вставки в мультимедийном потоке на основе сравнения коэффициентов полиномов, аппроксимируемых гистограммы изображений кадров с динамическим порогом принятия решения // Информационные системы и технологии. 2015. №1. С. 79–87.
26. *Grady L.* Random Walks for Image Segmentation // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2006. vol. 28. no. 11. pp. 1768–1783.
27. *Белим С.В., Ларионов С.Б.* Сегментация изображений на основе алгоритма выделения сообществ на графе // Математические структуры и моделирование. 2016. № 3(39). С. 74–85.
28. *Старожилова О.В.* Распознавание цифровых изображений методом построения поля направлений // Международный научно-исследовательский журнал. 2017. № 2(56). С. 135–137.
29. Official web site FantaMorph. URL: [www.fantomorph.com/index.html](http://www.fantomorph.com/index.html) (дата обращения: 15.02.2015).

**Орешин Андрей Николаевич** — к-т техн. наук, доцент, сотрудник, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: теория информации, теория графов, теория массового обслуживания, теория вероятностей, теория принятия решений, применение методов математического и имитационного моделирования в телекоммуникациях. Число научных публикаций — 67. [strongnuts@mail.ru](mailto:strongnuts@mail.ru); Приборостроительная, 35, Орел, 302034; р.т.: +7(4862)549500.

**Лысанов Иван Юрьевич** — сотрудник, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: теория вероятностей, теория графов, теория массового обслуживания, теория принятия решений, применение методов математического моделирования в телекоммуникациях, имитационное моделирование, компьютерная обработка изображений и цифровых сигналов, прикладное программирование. Число научных публикаций — 27. [IvanLisanov@yandex.ru](mailto:IvanLisanov@yandex.ru); Приборостроительная, 35, Орел, 302034; р.т.: +7(4862)549500

A.N. ORESHIN, I.YU. LISANOV  
**A NEW METHOD FOR AUTOMATION OF THE PERSONNEL  
 AUTHENTICATION PROCESS USING A VIDEO STREAM**

---

*Oreshin A.N., Lisanov I.Yu.* **A New Method for Automation of the Personnel Authentication Process Using a Video Stream.**

**Abstract.** On the basis of research carried out on automated control systems for industrial enterprises (ICS), the work proposes a mathematical model for the authentication of personnel using the technology of generation and processing of a heterogeneous stream containing photographic identification signs of personnel from video surveillance sources in the traffic of video data. A distinctive feature of the model are navigation operators and outputs to signal processing according to aggregate stream video management, allocation of frame-inserts bearing photographic identification signs, segmentation of space images required for authentication of staff in integrated access control system, as well as the use of technologies to restore the video stream. A technique for identifying frames-inserts in heterogeneous video stream has been developed, which is based on the estimation of total differential extreme brightness of frame-folds and an analysis of the histograms of image frames according to the correlation coefficients and polynomials of Chebyshevskii approximation. This technique uses dynamic threshold for authentication of frames and making a decision about their class on the basis of a majority method of data processing. The paper presents the results of simulation of the process of personnel authentication on the basis of the proposed model and methodologies, allowing one to estimate efficiency of visual personnel authentication, meeting the requirements of the reliability of decision making and limiting the transmission capacity of the data network.

**Keywords:** access control system, video surveillance system, model, heterogeneous and aggregated flows of data, identification sign (biometric, code and photographic), frame-insertion, authentication of personnel.

---

**Oreshin Andrey Nikolaevich** — Ph.D., associate professor, researcher, The Academy of Federal Security Guard Service of the Russian Federation. Research interests: information theory, graph theory, a waiting-line theory, theory of chances, decision principle, methods of mathematic and imitational modeling application in telecommunication. The number of publications — 67. strongnuts@mail.ru; 35, Priborostroitel'naya str., Orel, 302034, Russia; office phone: +7(4862)549500.

**Lisanov Ivan Yurevich** — сотрудник, Академия Федеральной службы охраны Российской Федерации. Research interests: probability theory, graph theory, queueing theory, decision theory, decision principle, application of mathematical simulation methods in telecommunications, simulation modeling, computer processing of images and digital signals, application programming. The number of publications — 27. IvanLisanov@yandex.ru; 35, Priborostroitel'naya Street, Orel, 302034, Russia; office phone: +7(4862)549500.

## References

1. Kozachok A.V., Bochkov M.V., Fatkueva R.R., Tuan L.M. [Analytical model for protecting documentary file formats from unauthorized access]. *Trudy SPIIRAN – Proceedings of SPIIRAS*. 2015. vol. 6(43). pp. 228–252. (In Russ.).

2. GOST R ISO/IEC 9594-8-98 [Information technology. Open Systems Interconnection. Reference book. Part 8. Authentication basics]. M.: Gosstandart Rossii. 2001. (In Russ.).
3. Novak T., Gerstinger A. Safety and Security-Critical Services in Building Automation and Control Systems. *IEEE Industrial Electronics*. 2010. vol. 57. pp. 3614–3621.
4. Oficial'nyj sajt kompanii PERCo [Official web site of the company PERCo]. Available at: [www.perco.ru](http://www.perco.ru). (accessed 17.08.2015). (In Russ.).
5. Oficial'nyj sajt kompanii Anviz Biometric Inc [Official web site of the company Anviz Biometric Inc] Available at: [www.anviz.com](http://www.anviz.com). (accessed 6.05.2015). (In Russ.).
6. Ibrahim R., Zin Z. Study of automated face recognition system for office door access control application. IEEE 3rd International Conference on Communication Software and Networks (ICCSN). 2011. pp. 132–136.
7. Lapina T.I., Epishev N.N., Lapin D.V. [Method for biometric authentication of the user in access control systems]. *Trudy SPIIRAN – Proceedings of SPIIRAS*. 2013. vol. 4(27). pp. 189–199. (In Russ.).
8. Park J., Lin S. A random effect model for reconstruction of spatial chromatin structure. *Biometrics journal of the International Biometric Society*. 2017. vol. 73. no. 1. pp. 52–62.
9. Shen C. et al. Identification of subpopulations with distinct treatment benefit rate using the Bayesian tree. *Biometrical Journal*. 2016. vol. 58. no. 6. pp. 1357–1375.
10. Bytrina A.V., Bygaeva A.P. [Biometric identification]. *Aktual'nie problemi aviathii i kosmonavtika – Actual problems of aviation and cosmonautics*. 2012. vol. 8. pp. 389–390. (In Russ.).
11. Cekhanovskiy V.V., Chertovsky V.D. [Mathematical modeling of local regulation of blood flow]. *Vestnik Nizhnegorodckogo gosydarstvennogo univertsiteta – Bulletin Nizhnevartovsk State University*. 2014. vol. 3. pp. 86–95. (In Russ.).
12. Oreshin A.N., Oreshin N.A., Shumilin V.S., Panchyuk P.V. [Methodology of optimal channels distribution and highways based on the determination of productive ways by using the automated control systems of communication]. *Telekommunikathii – Telecommunications*. 2016. vol. 10. pp. 44–48. (In Russ.).
13. Vizil'ter Yu. et al. *Obrabotka i analiz tsifrovih izobrazhenii c primerami na LabVIEW i IMAQ Vision* [Digital images processing and analysis with examples in LabVIEW and IMAQ Vision]. Moscow: DMK Press. 2008. 464 p. (In Russ.).
14. Kharinov M.V. [Model of Digital Image Attributed with Virtual Memory Basing on Pseudo-Ternary Number System]. *Trudy SPIIRAN – Proceedings of SPIIRAS*. 2007. vol. 4. pp. 126–135. (In Russ.).
15. Tregubov R.B., Aleksikov Yu.G., Saitov S.I. [Representation of the hierarchical multilayer routing systems in a set-theoretic base]. *Trudy SPIIRAN – Proceedings of SPIIRAS*. 2016. vol. 1(44). pp. 139–168. (In Russ.).
16. Tregubov R.B., Saitov I.A. *Teoreticheskie osnovy analiza i optimizatsii ierarkhicheskikh mnogourovnevnykh marshrutiziruyushchikh system* [The theoretical framework for the analysis and optimization of hierarchical multilayer routing systems]. Orel: Akademiya FSO Rossii. 2016. 585 p. (In Russ.).
17. Salnikov I.I., Martens-Atushev D.S. [Digital image processing techniques]. *Mezhdynarodnii stydencheskii naychnii vestnik – International student research bulletin*. 2015. vol. 3–2. pp. 276–277. Available at: [www.eduherald.ru](http://www.eduherald.ru). (accessed 04.03.2017). (In Russ.).
18. Gonsales R., Vuds R., Chochia P.A. *Mir tsifrovoi obrabotki. Tsifrovaia obrabotka izobrazhenii* [World of the digital processing. Digital Image Processing]. Moscow: Tehnosfera Publ. 2006. 1072 p. (In Russ.).
19. Shapiro L.G., Stockman G.C. *Computer Vision*. New Jersey. Prentice-Hall. 2001. pp. 279–325.

20. Oreshin A.N., Saitov I.A., Oreshin N.A. [Strategy of the Video Communication Services Quality Enhancement Based on the Filtration of a Video Stream Containing Snap-Insertions with Information Noise]. *Trudy SPIIRAN – Proceedings of SPIIRAS*. 2015. vol. 4(41). pp. 57–81. (In Russ.).
21. Kharinov M.V., Hanikov I.G. [The combined method of improving image segmentation]. *Vestnik Byriatskogo gosydarstvennogo univertsiteta. Seria. Matematika i informatika – Bulletin Buryat State University. Mathematic and informatization series*. 2015. vol. 9. pp. 118–124. (In Russ.).
22. Kormen T., Lejzerson Ch., Rivest R., Shtajn K. *Algoritmi: postroenie i analiz. 3 izdanie* [Algorithms: design and analysis]. Moscow: "Vil'jams". 2013. 1323 p. (In Russ.).
23. Oreshin A.N., Skurnovich A.V., Kiryuhin D.A. [Method of frame authentication of multimedia data flow based on cross-correlation analysis of histograms of frame images]. Patent RF. no. 2506640. 2014. (In Russ.).
24. Oreshin A.N., Lysanov I.Yu. [Snap-insertion identification procedure in a video data stream based on the correlative analysis of the histograms of snap images with a dynamic threshold of decision making]. *Informacionnye sistemy i tehnologii – Information systems and technologies*. 2014. vol. 6. pp. 129–138. (In Russ.).
25. Lisanov I.Yu., Oreshin A.N. [Authentication of frame-insertion in a multimedia stream based on comparison of coefficients of the polynomials approximated histograms of frame images with the dynamic making decision threshold]. *Informacionnye sistemy i tehnologii – Information systems and technologies*. 2015. vol. 1. pp. 79–87. (In Russ.).
26. Grady L. Random Walks for Image Segmentation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2006. vol. 28. no. 11. pp. 1768–1783.
27. Belim S.V., Larionov S.B. [Segmentation of images the basis of algorithm of communities separation on the graph]. *Matematicheskie stryktury i modelirovanie – Mathematical structures and modeling*. 2016. vol. 3(39). pp. 74–85. (In Russ.).
28. Starozhilova O.V. [Recognition of digital images by means of directional field construction]. *Mezhdynarodnii naychno-issledovatel'skii zhyrnal – International research journal*. 2017. vol. 2(56). pp. 135–137. (In Russ.).
29. Official web site FantaMorph. Available at: [www.fantomorph.com/index.html](http://www.fantomorph.com/index.html) (accessed 15.02.2015).