

# Защищенное исполнение нейросетевых алгоритмов классификации образов для задач биометрической аутентификации на базе сетей корреляционных нейронов

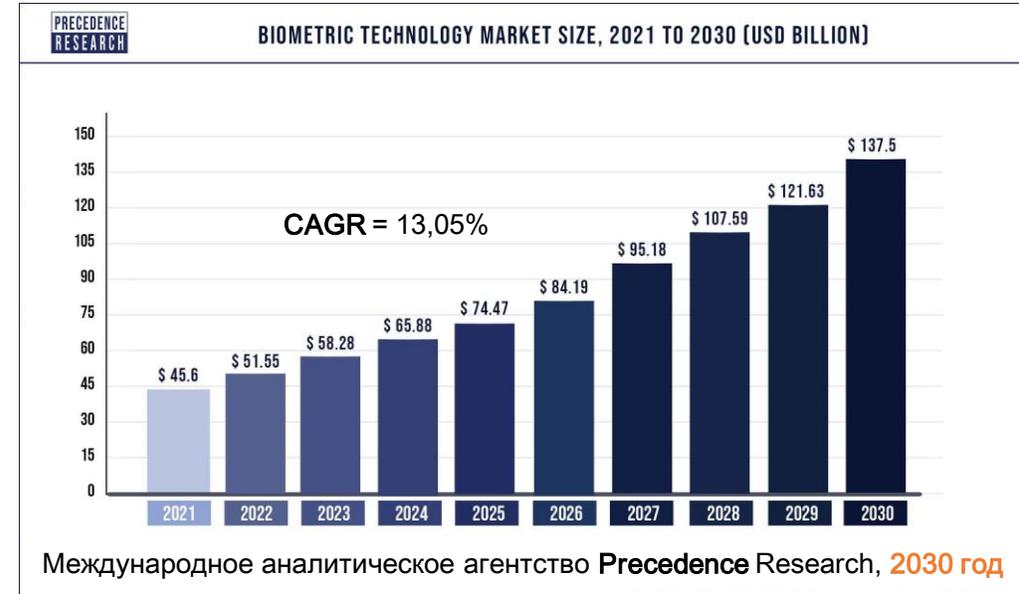
Работа выполнена ОмГТУ в рамках государственного задания Минобрнауки России на 2023-2025 годы № FSGF-2023-0004

**Сулавко Алексей Евгеньевич**

д.т.н., доцент кафедры комплексной защиты информации, главный научный сотрудник, **ФГАОУ ВО ОмГТУ**



## Объем мирового рынка биометрических систем



Прогноз объемов мирового рынка от Transparency Market Research на 2031 год:

- рынок биометрии достигнет объема \$136,18 млрд. (CAGR = 13,3%)
- сегмент биометрических платежных систем достигнет \$8,8 млрд. (CAGR = 56,2%)
- сегмент лицевой биометрии достигнет \$20,5 млрд.
- сегмент бесконтактной и многофакторной биометрической аутентификации – \$59,5 млрд.
- крупные инвестиции направлены на сегменты голосовой и лицевой биометрии

- Подверженность компьютерным атакам
- Компрометация знаний ИИ (биометрических образов)
- Сложность автоматизации обучения на малых выборках
- Низкая робастность обучения
- Недостаточная надежность\*

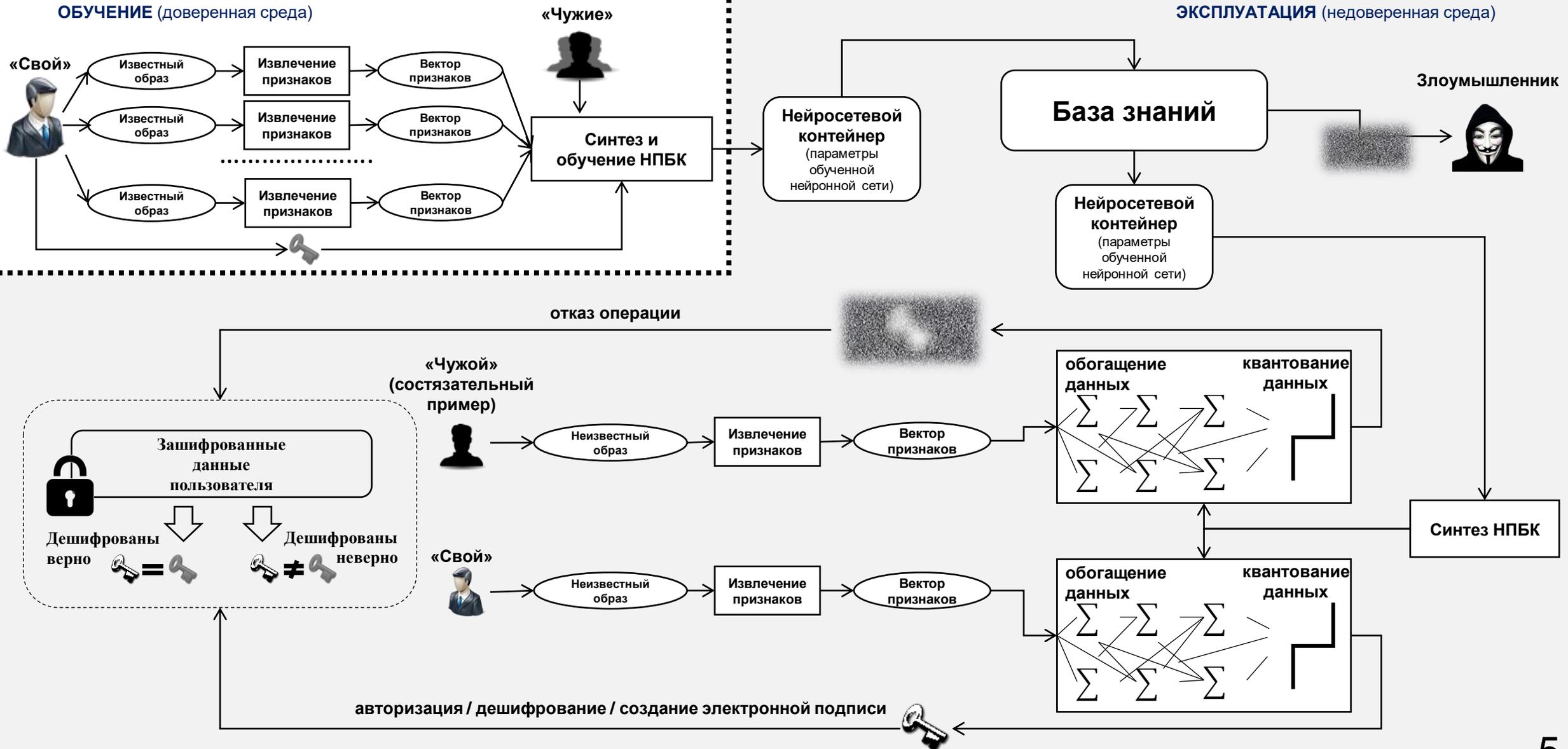
\*недостаточные показатели вероятностей «ложного отказа» **FRR** и «ложного допуска» **FAR** или неспособность системы сохранять их с течением времени на приемлемом уровне



# Защищенное исполнение нейросетевых алгоритмов доверенного ИИ

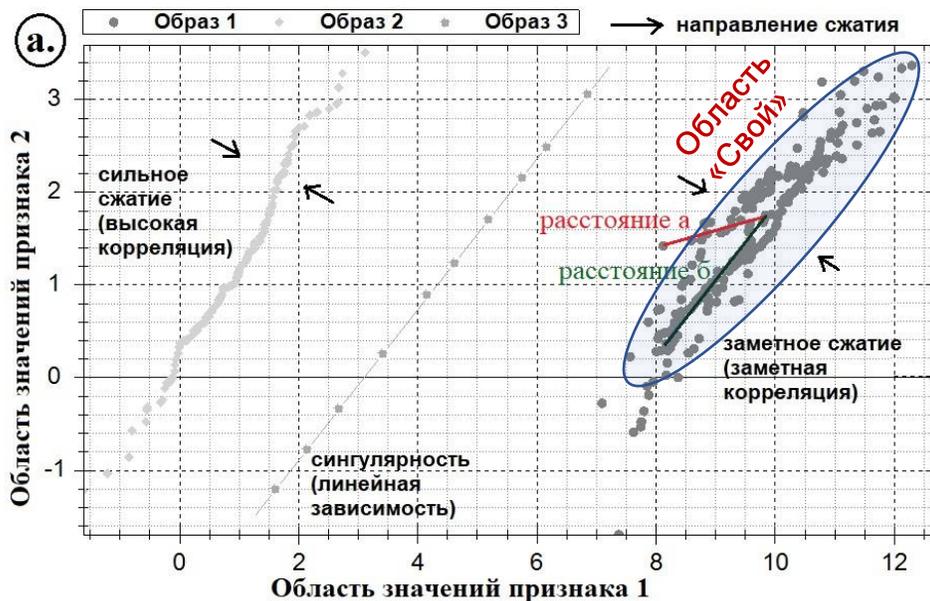


# Нейросетевые преобразователи биометрия-код (НПБК)

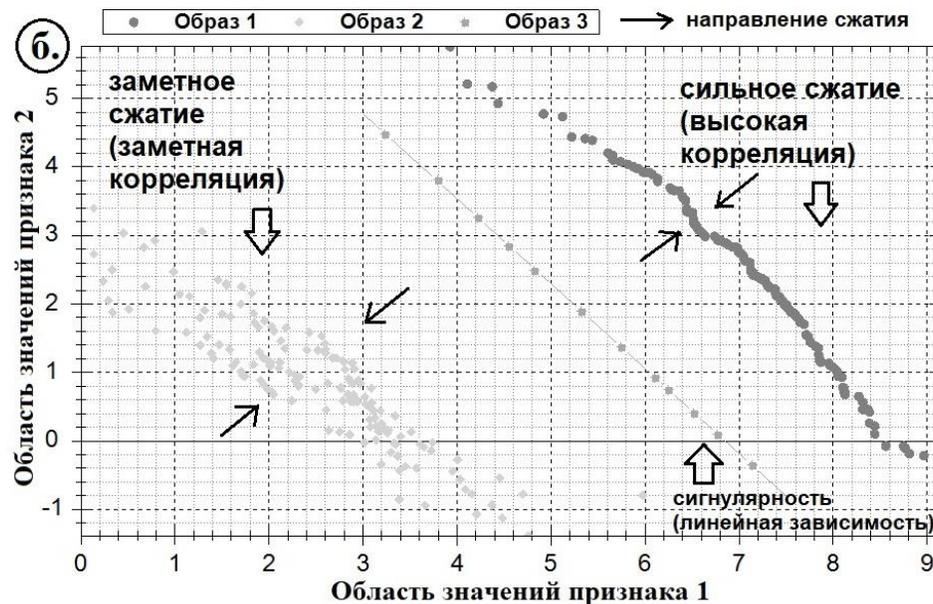


# Искавление пространства признаков из-за корреляции между измерениями

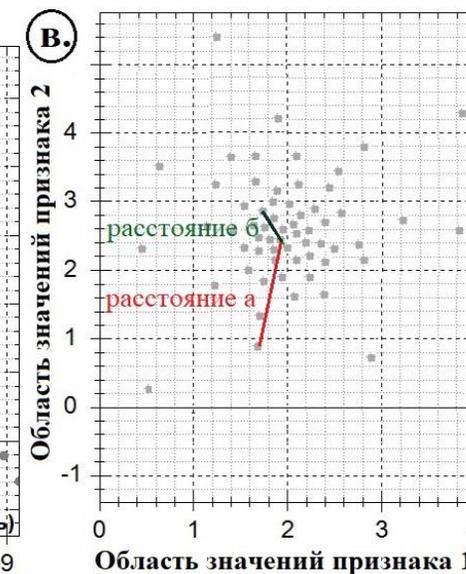
а. при положительной корреляции между признаками



б. при отрицательной корреляции



в. при независимости признаков



$$y = \sqrt[g]{\sum_{j=1}^n \left| \frac{(m_j - a_j)}{\sigma_j} \right|^g}$$

где  $a_j$  – значение  $j$ -го признака;  $n$  – количество признаков;

$m_j$  и  $\sigma_j$  – математическое ожидание и среднеквадратичное отклонение значений  $j$ -го признака для класса «Свой», с которым сравнивается образ  $\bar{a}$  (класс «Свой» представляет биометрические образы одного из легитимных пользователей);

$g$  – степенной коэффициент, определяющий уровень «искавления» пространства.

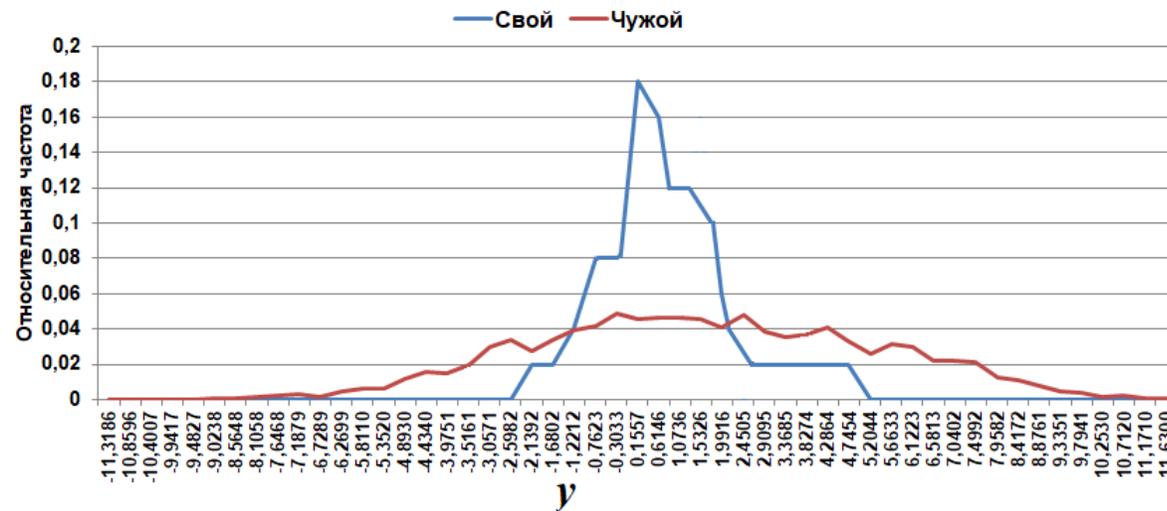
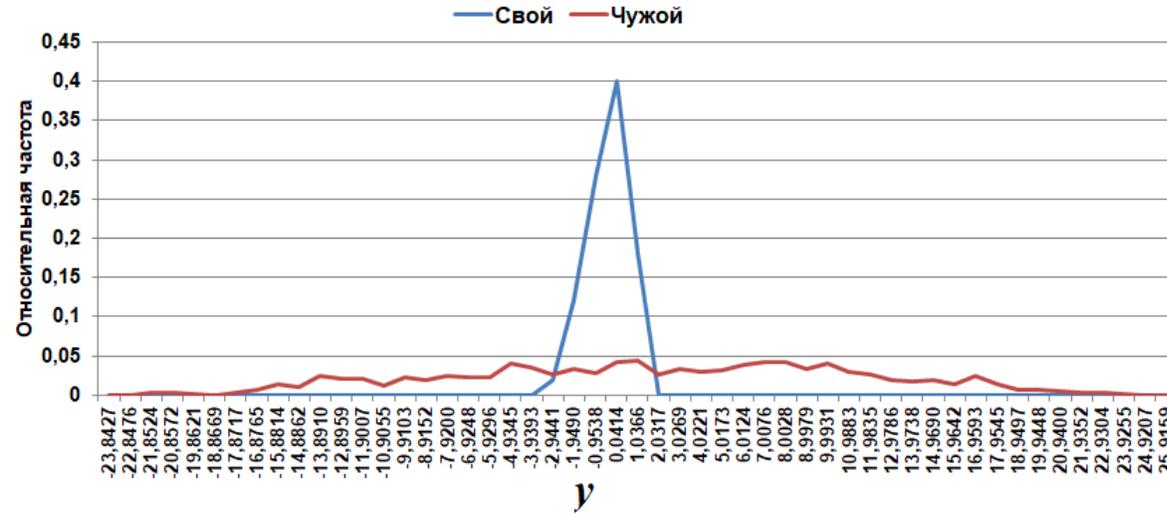


Рисунок – Графики относительных частот значений меры (1) при  $g = 1$ ,  $n' = 5$ :  
 сверху – для случая сильно зависимых признаков ( $C_{j,t} > 0,7$ );  
 внизу – для случая независимых признаков ( $|C_{j,t}| < 0,3$ ).

$$y = \sqrt[g]{\sum_{j=1}^n \left| \frac{m_t - a_t}{\sigma_t} \right|^g - \left| \frac{m_j - a_j}{\sigma_j} \right|^g}, j \neq t, \quad (1)$$

$$y = \sum_{j=1}^n \left| \frac{a_t}{\delta_t} \right|^g - \left| \frac{a_j}{\delta_j} \right|^g, j \neq t, \quad (2)$$

$$y = \sqrt{\frac{1}{n} \sum_{j^*=1}^n (a'_{j^*} - m')^2}, m' = \frac{1}{n} \sum_{t^*=1}^n a'_{t^*} \quad (3)$$

где  $a_j$  – значение  $j$ -го признака;

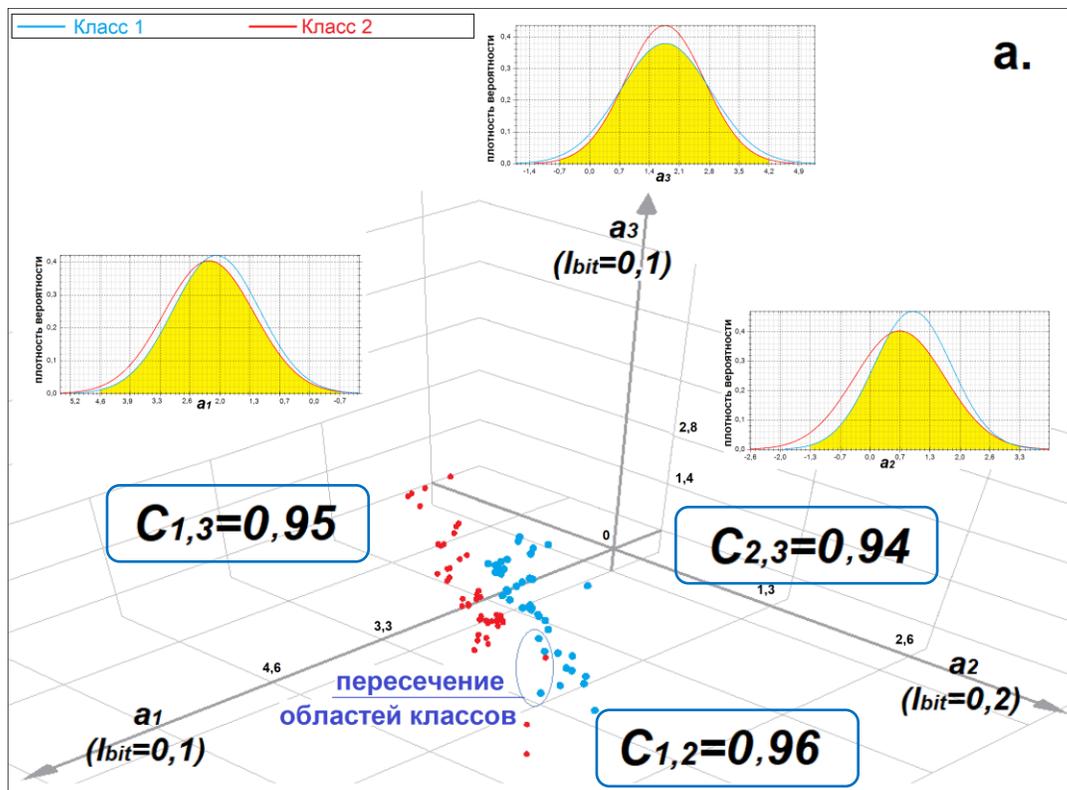
$n$  – количество признаков;

$m_j$  и  $\sigma_j$  – математическое ожидание и среднеквадратичное отклонение значений  $j$ -го признака для класса «Свой», с которым сравнивается образ  $\bar{a}$ ;

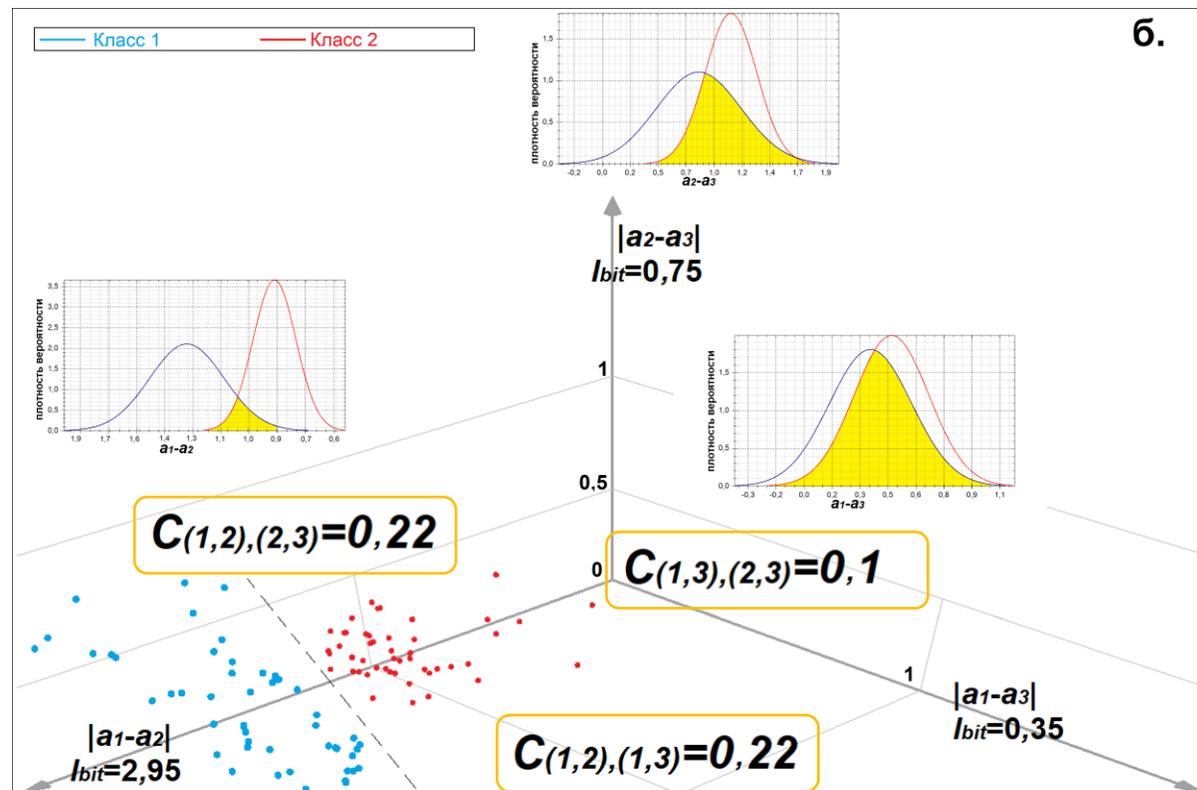
$\mu_j$  и  $\delta_j$  – это нормирующие коэффициенты, вычисляемые как мат. ожидание и стандартное отклонение значений признака для класса «Чужие»;

$g$  – степенной коэффициент, определяющий уровень «искривления» пространства.

а. положительно коррелированных признаков



б. мета-признаков, производных от исходных признаков



$$a'_{j*} = a'_{t,j} = f(a_t, a_j) = \left| \frac{a_t}{\delta_t} \right|^g - \left| \frac{a_j}{\delta_j} \right|^g, \quad (1)$$

$$j > t, j^* = \sum_{t^*=1}^{t-1} (n - t^*) + j - t \quad (2)$$

$$n' = 0,5(n(n-1)) = 0,5n^2 - 0,5n \quad (3)$$

где  $\delta_j$  – это нормирующий коэффициент, вычисляемый как среднее квадратичное отклонение значений  $j$ -го признака для класса «Чужие»

$C_{j,t}$  – это коэффициент парной корреляции между признаками под номерами  $j$  и  $t$

# Модель корреляционного нейрона первого поколения

$$y = \sqrt{\frac{1}{\eta} \sum_{i=1}^{\eta} w_i (a'_i - m')^2}, m' = \frac{\sum_{i=1}^{\eta} a'_{i^*}}{\eta} \quad (1)$$

$\eta$  – количество входов нейрона,  $w_i$  – вес  $i$ -го синапса ( $w_i > 0$ )

$$w_i = \frac{|m''_{(G),i} - m''_{(I),i}|}{\sigma''_{(G),i} \cdot \sigma''_{(I),i}}, \quad (2)$$

$m''_{(G),i}, m''_{(I),i}$  – математические ожидания,

$\sigma''_{(G),i}, \sigma''_{(I),i}$  – стандартные отклонения  $i$ -го мета-признака

2-го порядка (3) для образов «Свой» и «Чужие», соответственно

$$a''_i = (a'_i - m')^2 \quad (3)$$

После обучения параметры  $m''_{(G),i}, m''_{(I),i}, \sigma''_{(G),i}, \sigma''_{(I),i}$  удаляются.

**Активация нейрона (4):**

$$\phi(y) = \begin{cases} 3, & y < T_{left} \\ 2, & T_{left} \leq y < T_{middle} \\ 1, & T_{middle} \leq y < T_{right} \\ 0, & y \geq T_{right} \end{cases}, \quad (4)$$

$T_{left}, T_{middle}$  и  $T_{right}$  – левый, средний и правый пороги активации

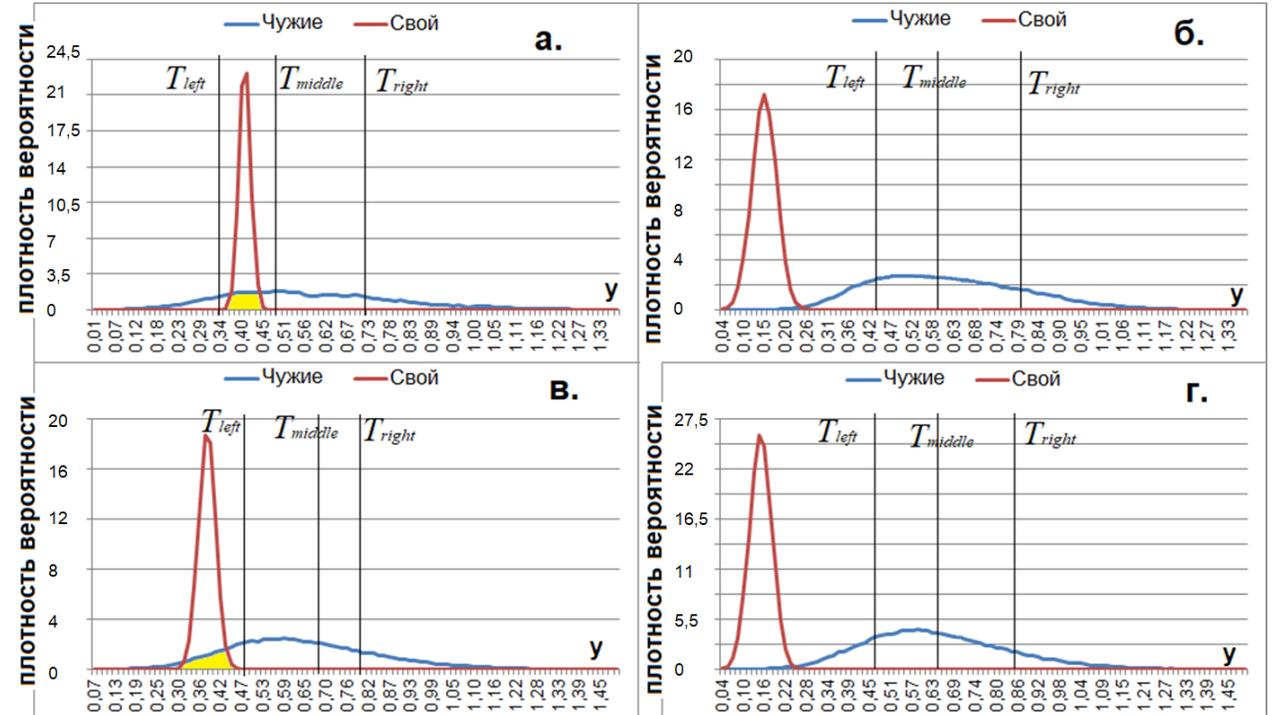


Рисунок – Графики плотностей вероятности значений меры (1) для сгенерированных данных при  $g=1, I \approx 1,75$  бит:

а. для всех классов  $1 > C_{j,t} > 0,95, n'=10$ ;

б. для всех классов  $-1 < C_{j,t} < -0,95, n'=10$ ;

в. для классов «Свой»  $1 > C_{j,t} > 0,95$ , для класса «Чужие»  $|C_{j,t}| < 0,3, n'=10$ ;

г. для классов «Свой»  $-1 < C_{j,t} < -0,95$ , для класса «Чужие»  $|C_{j,t}| < 0,3, n'=10$ ;

# Преимущества и недостатки модели корреляционных нейронов первого поколения



Преимущества по сравнению с ГОСТ Р 52633.5	Гипотетический недостаток
<b>Более высокая длина ключа</b> (по результатам экспериментов может многократно превышать длину ключа для НПБК, обученного по ГОСТ Р)	<b>Заявлена потенциальная атака</b> , обнародованная в рамках РусКрипто 2023 (авторы: Маршалко Г.Б., Романенков Р.А., Труфанова Ю.А., ТК26)
<b>Более высокая надежность решений</b> (ниже FRR и FAR)	Нейрон не поддерживает работу <b>со слабо коррелированными парами признаков</b> (необходимо наличие достаточного количества сильно коррелированных признаков)

**На базе первой модели корреляционных нейронов создана первая редакция стандарта** ГОСТ Р «Искусственный интеллект. Нейросетевые алгоритмы в защищённом исполнении. Автоматическое обучение нейросетевых моделей на малых выборках в задачах классификации»

**Нейро-корреляционный преобразователь (НКП)** – нейросетевой преобразователь образов в код на основе сети корреляционных нейронов

# Несостоятельность атаки на НКП на базе корреляционных нейронов предыдущего поколения



## 1. Неверное допущение:

Предполагается, что у нарушителя есть набор примеров из различных классов «Свой», при этом среди них есть один, который использовался для обучения доступного нарушителю НКП

## 2. Некорректный критерий сходства между двумя НКП и, как следствие, некорректные действия атакующего:

- Атакующий пытается обучить несколько НКП путем вычисления весовых коэффициентов и нахождения пороговых значений (границ)  $T_{left}$ ,  $T_{middle}$ ,  $T_{right}$ , **не учитывая номера хеш-таблиц.**
- Далее он пытается выбрать среди обученных НКП тот, у которого границы ближе всего по некоторой метрике к границам атакуемого нейрона. При этом **различие весовых коэффициентов двух НКП не берется во внимание.**
- **Атакующий строит метрику сходства НКП целиком на близости границ, а нужно строить на сходстве выходных состояний нейронов.**

Схожесть границ  $T_{left}$ ,  $T_{middle}$ ,  $T_{right}$  у двух НКП не свидетельствует о том, что у этих НКП область «Свой» будет находиться на идентичных интервалах:

$$[-\infty; T_{left}], \quad [T_{left}; T_{middle}], \quad [T_{middle}; T_{right}], \quad [T_{right}; \infty]$$

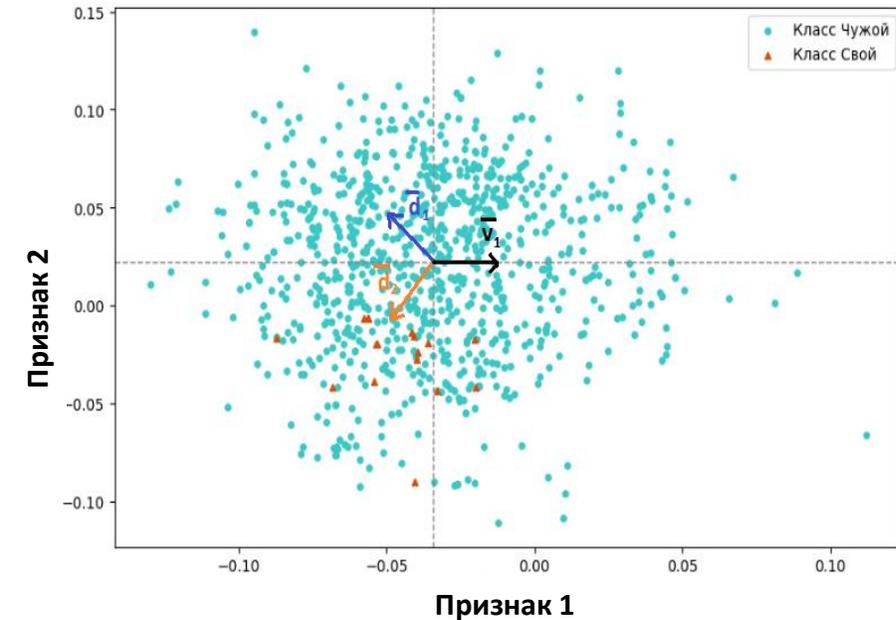
В описании атаки не приводится свидетельств того, что фальсифицированный и легитимный НКП будут генерировать схожие или идентичные выходные коды в ответ на одинаковые входные образы.

Не показана корреляция между значением критерия и правильным выбором интервала.

## 3. Не понятно, какое количество нейронов использовано в рамках атаки на НКП.

Итог: **выводы авторов преждевременны**, предложенный авторами критерий не позволяет корректно определять входные данные, использовавшиеся для обучения атакуемого НКП.

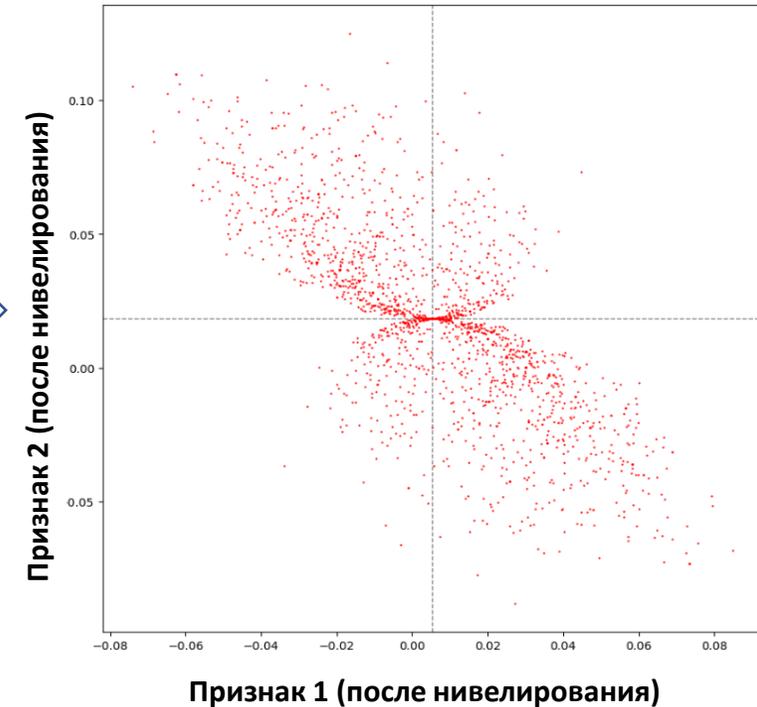
# Драфт второй модели корреляционного нейрона для работы со слабо коррелированными признаками (разработана Панфиловой И.Е.)



*Евклидовы расстояния от центра  
«Все Чужие» до образа  
определенного класса ( $d_2$ ) и  
случайного образа ( $d_1$ )  
в пространстве исходных признаков*

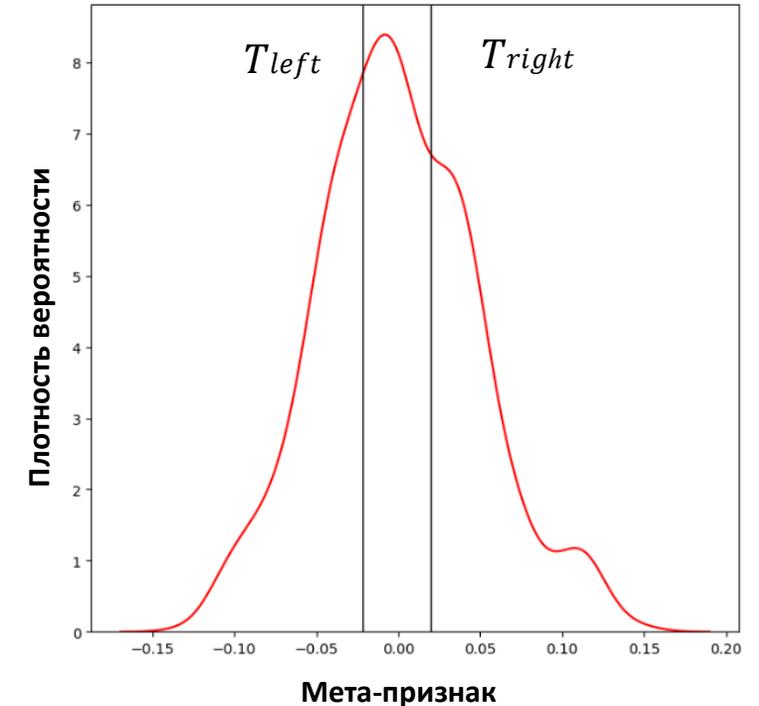
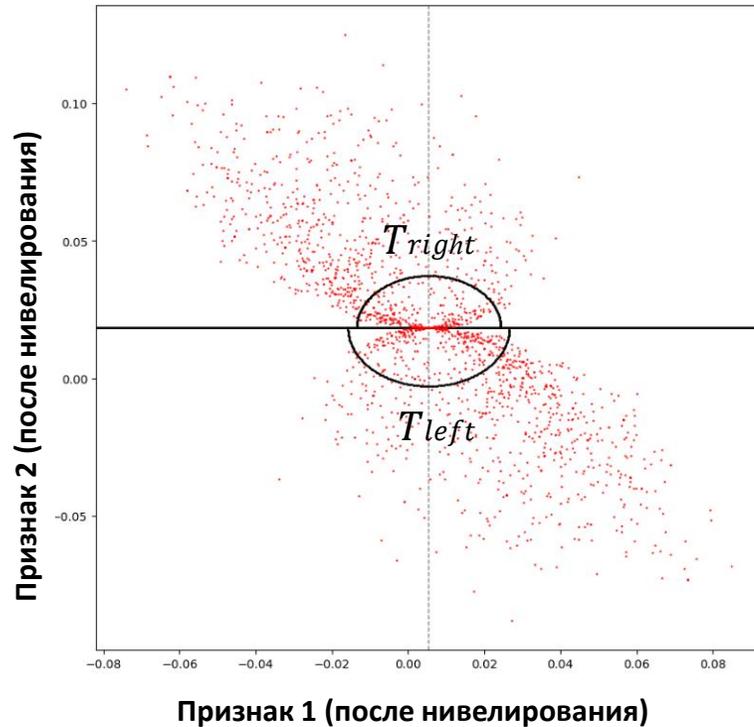
$$a'_{i,j} = \sqrt{(a_i - m_i)^2 + (a_j - m_j)^2} * \sin(\widehat{\vec{d}, \vec{v}}) \quad (1)$$

тригонометрическое  
нивелирование



*Мета-пространство,  
порождаемое метрикой (1)*

# Драфт второй модели корреляционного нейрона для работы со слабо коррелированными признаками (разработана Панфиловой И.Е.)



Визуализация порогов  
в мета-пространстве признаков

Визуализация порогов на графике  
функции плотности вероятности  
распределения мета-признаков (1)

Евклидово расстояние, скорректированное путем  
тригонометрического нивелирования, – это **новый мета-признак (1)**

$$a'_{i,j} = \sqrt{(a_i - m_i)^2 + (a_j - m_j)^2} * \sin(\widehat{d, \vec{v}}) \quad (1)$$

# Драфт второй модели корреляционного нейрона для работы со слабо коррелированными признаками (разработана Панфиловой И.Е.)

Функционал нейрона:

$$y = \sum_{i=1}^n \sqrt{(a_i - m_i)^2 + (a_j - m_j)^2} * \sin(\widehat{d}, \widehat{v}), i \neq j \quad (2)$$

Функция активации нейрона:

$$\phi(y) = \begin{cases} 1, & y < T_{left} \\ 0, & T_{left} \leq y < T_{right}, \\ -1, & y \geq T_{rightt} \end{cases} \quad (3)$$

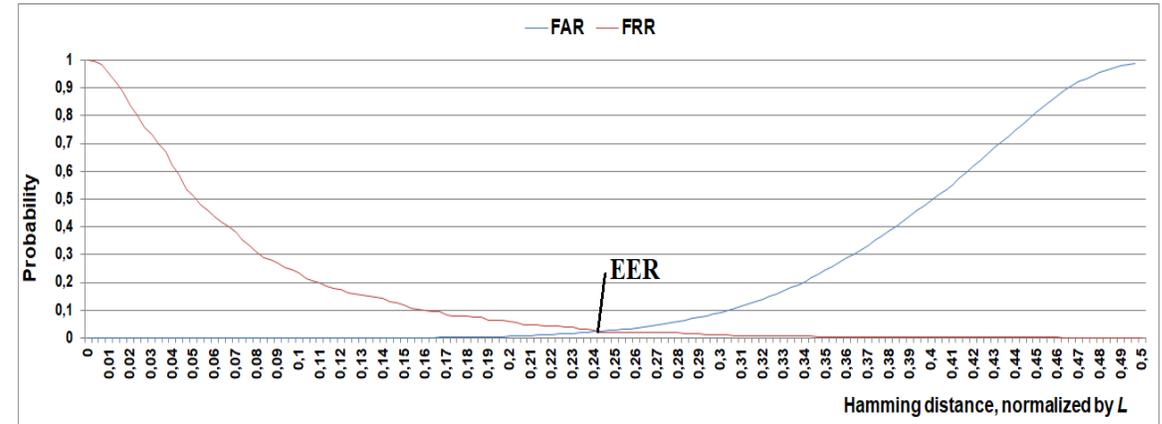
Хеш- таблица №	-1	0	1	№	-1	0	1
1	11	00	01	13	01	00	11
2	11	00	10	14	01	00	10
3	11	01	00	15	01	10	00
4	11	01	10	16	01	10	11
5	11	10	00	17	01	11	10
6	11	10	01	18	01	11	00
7	00	01	11	19	10	00	01
8	00	01	10	20	10	00	11
9	00	10	01	21	10	01	11
10	00	10	11	22	10	01	00
11	00	11	10	23	10	11	00
12	00	11	01	24	10	11	01

# Предварительные результаты экспериментов с моделями (выполнено Панфиловой И.Е.)



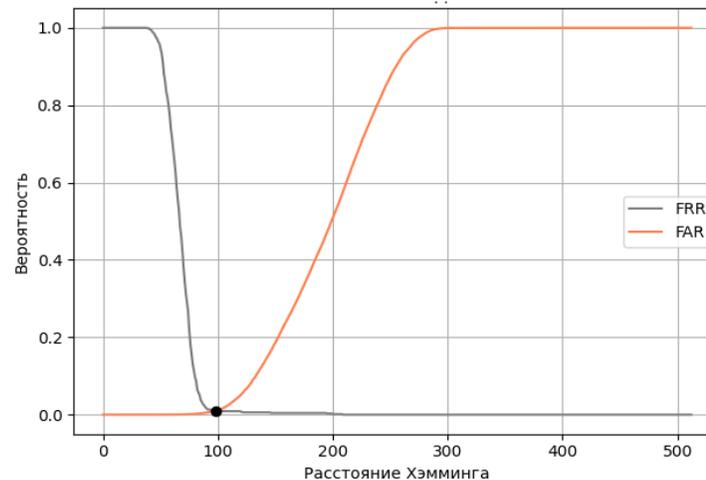
**Первая модель**  
(распознавание по эхограммам ушного канала):

AIC-ears-75 (EER = 0,0238%):

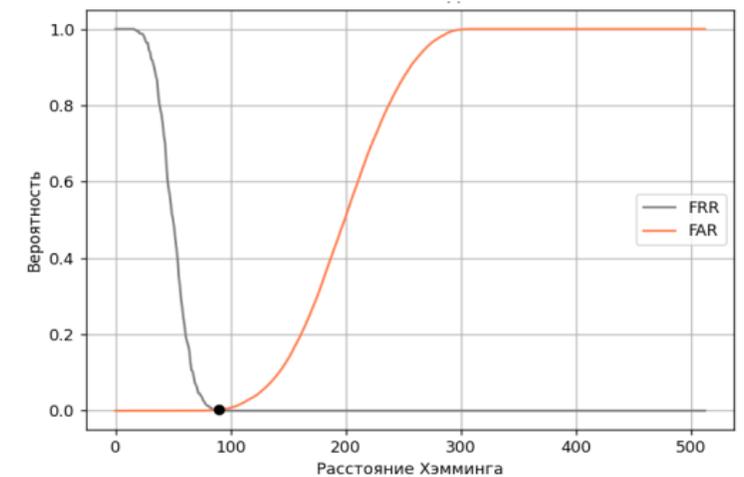


**Вторая модель**  
(распознавание по лицу):

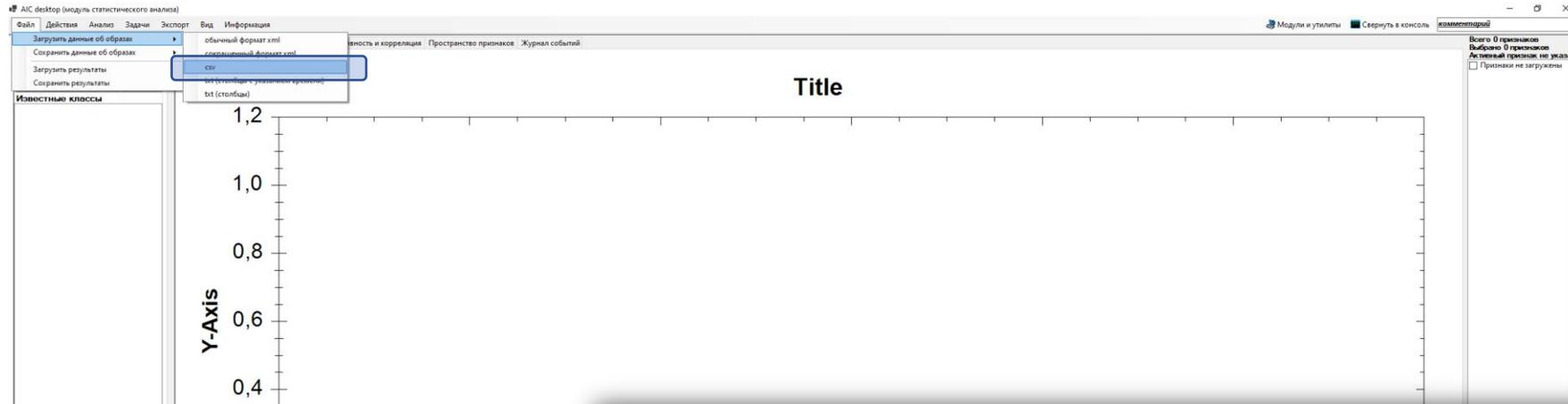
Labeled Faces in the Wild (EER = 0,012%):



Faces94 (EER = 0,003%):



# AIC desktop



# AIC desktop



Нейросетевая обработка данных, Нейросетевая обработка данных

Файл Действия Анализ Задачи Экспорт Вид Информация

Описания классов Шаблоны

Выбрать образы равномерно

Инвертировать выбор образы

Выбор сгенерированные

**Известные классы (24)**

- \_enrol\_f0002\_271.pcm,28
- \_enrol\_f0002\_272.pcm,24
- \_enrol\_f0002\_273.pcm,25
- \_enrol\_f0002\_274.pcm,24
- \_enrol\_f0002\_275.pcm,23
- \_enrol\_f0002\_276.pcm,24
- \_enrol\_f0002\_277.pcm,25
- \_enrol\_f0002\_278.pcm,25; Всего ре
- \_enrol\_f0002\_279.pcm,24; Всего ре
- \_enrol\_f0002\_280.pcm,23; Всего ре
- \_enrol\_f0004\_371.pcm,11; Всего ре
- \_enrol\_f0004\_372.pcm,16; Всего ре
- \_enrol\_f0004\_373.pcm,13; Всего ре
- \_enrol\_f0004\_374.pcm,14; Всего ре
- \_enrol\_f0004\_375.pcm,12; Всего ре
- \_enrol\_f0004\_376.pcm,12; Всего ре
- \_enrol\_f0004\_377.pcm,15; Всего ре
- \_enrol\_f0004\_378.pcm,11; Всего ре
- \_enrol\_f0004\_379.pcm,17; Всего ре
- \_enrol\_f0004\_380.pcm,12; Всего ре
- \_enrol\_f0005\_441.pcm,13; Всего ре
- \_enrol\_f0005\_442.pcm,13; Всего ре
- \_enrol\_f0005\_443.pcm,13; Всего ре
- \_enrol\_f0005\_444.pcm,13; Всего ре
- \_enrol\_f0005\_445.pcm,13; Всего ре
- \_enrol\_f0005\_446.pcm,13; Всего ре
- \_enrol\_f0005\_447.pcm,13; Всего ре
- \_enrol\_f0005\_448.pcm,13; Всего ре
- \_enrol\_f0005\_449.pcm,13; Всего ре
- \_enrol\_f0005\_450.pcm,13; Всего ре
- \_enrol\_f0006\_461.pcm,17; Всего ре
- \_enrol\_f0006\_462.pcm,17; Всего ре v

Кол-во реал. 10 Снять флажки

Выбрать все классы Выбрать образы Переместить выбранные

Кол-во реал. 1 Снять флажки

**Неизвестные классы (1)**

\_Impostor; Всего реализаций: 1890

Перейти в МЕТА-ПРОСТРАНСТВО ВЫБРАННЫХ признаков

Определить/исключить некорректные реализации выбранных классов F2

Настроить метод определения/исключения грубых ошибок в данных

**ОБУЧИТЬ - сформировать эталоны выбранных классов F3**

из ВСЕХ образов, кроме 2-х (оставить по 2 образа для тестирования на каждый класс) Ctrl+F3

из шаблонов признаков SHIFT+F3

Информация об эталонах Ctrl+F1

Удалить эталоны Alt+F3

СГЕНЕРИРОВАТЬ ОБРАЗЫ на основе параметров созданных эталонов

НАЧАТЬ МОДЕЛИРОВАНИЕ КЛАССИФИКАЦИИ

ПРОСМОТР РЕЗУЛЬТАТОВ КЛАССИФИКАЦИИ F9

Спрятать/показать опции SHIFT+F1

Method определения грубых ошибок в данных: 1. Вычисление корреляции между образами

Модель/метод обучения (тип эталонов): 10. С-леуго-extractor (НПБК с защитой знаний на базе корреляционных нейронов)

Классификатор/решающее правило: 9. АДАПТЕР-ПБК (мера Хемминга, бинарные векторы)

Запоминать промежуточные решения

Использовать образы неизвестных классов в эксперименте

Сохранять историю эксперимента на диск

Изменять количество эталонов в процессе моделирования

Общие установки для процедур обучения, распознавания и поиска некорректных образов

Учитывать все признаки (иначе - только выбранные)

Применить выбранную последовательность признаков

Статус: планирование эксперимента

Идентификация  без обучающих примеров

Верификация  FAR - только неизвестные классы

## Настройки классификатора

Комитет (ансамбль) корреляционных нейронов Байеса-Минковского с автоматическим обучением. Каждый нейрон имеет 4 выходных состояния (каждый нейрон генерирует два бита ключа). Нормировка векторов признаков выполняется на тренировочной выборке Чужих (по одному примеру на каждого Другого). Пороги нейронов настраиваются на валидационной выборке Чужих (по одному примеру на каждого Другого). Количество нейронов, ориентированных на обработку отрицательной или положительной корреляции, примерно одинаково. Корреляционный нейросетевой контейнер можно размещать в открытом виде (предположительно, пока атак на извлечение знаний не предложено)

Название параметра	Минимальное значение	Максимальное значение	Описание	Задать значение	Использовать значение по-умолчанию (вместо заданного)
N	2	1000000	Количество нейронов. ПО-УМОЛЧАНИЮ: 128	2	<input checked="" type="checkbox"/>
n	2	10000000	Количество входов у каждого нейрона. ПО-УМОЛЧАНИЮ: 4	2	<input checked="" type="checkbox"/>
Min Cor	-1	-0,01	Минимальный порог отрицательной корреляции. ПО-УМОЛЧАНИЮ: -0,5	-1	<input checked="" type="checkbox"/>
Max Cor	0,01	1	Максимальный порог положительной корреляции. ПО-УМОЛЧАНИЮ: 0,5	0,01	<input checked="" type="checkbox"/>
Асимметрия нейронов	0	1000000	Насколько количество нейронов, настроенных на положительную или отрицательную корреляцию, может различаться. ПО-УМОЛЧАНИЮ: 10% от количества нейронов	0	<input checked="" type="checkbox"/>
Расширение порогов	0,001	1000	Коэффициент влияния на пороги нейронов (при 1 < расширяется интервал Хемминга и нейрон чаще пропускает Своего, но реже отвергает Чужого, при <1 интервал Хемминга сужается). ПО-УМОЛЧАНИЮ: 1 (влияния нет)	0,001	<input checked="" type="checkbox"/>
Нормализация по мат. ожиданиям	0	1	При 1 нормировка признаков по мат. ожиданию и среднеквадратичному отклонению Чужих. ПО-УМОЛЧАНИЮ: 0 (нормировка только по среднеквадратичному отклонению)	0	<input checked="" type="checkbox"/>
p	0,001	1000	Степенной коэффициент. ПО-УМОЛЧАНИЮ: 0,5	0,001	<input checked="" type="checkbox"/>
Удалять нестабильные нейроны (имитация ЗНК)	0	1000000	Балансировка порогов по равновероятности откликов на Чужих. Нейроны, стабильность выходов которых при поступлении на вход образов Чужих несбалансирована в соответствии с [0,1, 0,4], удаляются. Включается при значении 1, создается эффект повышения энтропии кодов Чужие (как в режиме ЗНК). ПО-УМОЛЧАНИЮ: 0 (не удалять)	0	<input checked="" type="checkbox"/>
Минимальная информативность (чем ниже, тем информативнее)	0,0001	1	Удалять нейроны, площадь пересечения плотностей вероятности откликов которых для образов Свой и Чужие, выше данного значения. Чем выше площадь, тем ниже информативность. ПО-УМОЛЧАНИЮ: 1 (нейроны не удаляются)	0,0001	<input checked="" type="checkbox"/>
Весы	0	1	При 1 автоматически вычисляются веса синапсов по формуле, при 0 - не вычисляются. ПО-УМОЛЧАНИЮ: 1	0	<input checked="" type="checkbox"/>
Чужие	1	1000000	Количество образов от каждого Чужого для вычисления коэффициентов нормирования, а также аналогичное количество образов от Чужих для вычисления порогов нейронов (обе подвыборки не пересекаются). ПО-УМОЛЧАНИЮ: 1	1	<input checked="" type="checkbox"/>

Внутренние параметры (для АДАПТЕРА):

нет параметров

Внутренние параметры (для АДАПТЕРА-ПБК):

нет параметров

OK

**Подробнее** о направлениях наших исследований вы можете узнать на **сайте AIC desktop**

---

**AIC desktop**



**Алексей Сулавко**  
(ОМГТУ), д.т.н.

**AIC Platform**



**Контакты:**

**[sul@aiconstructor.ru](mailto:sul@aiconstructor.ru)**

**+7 953 394-90-54**

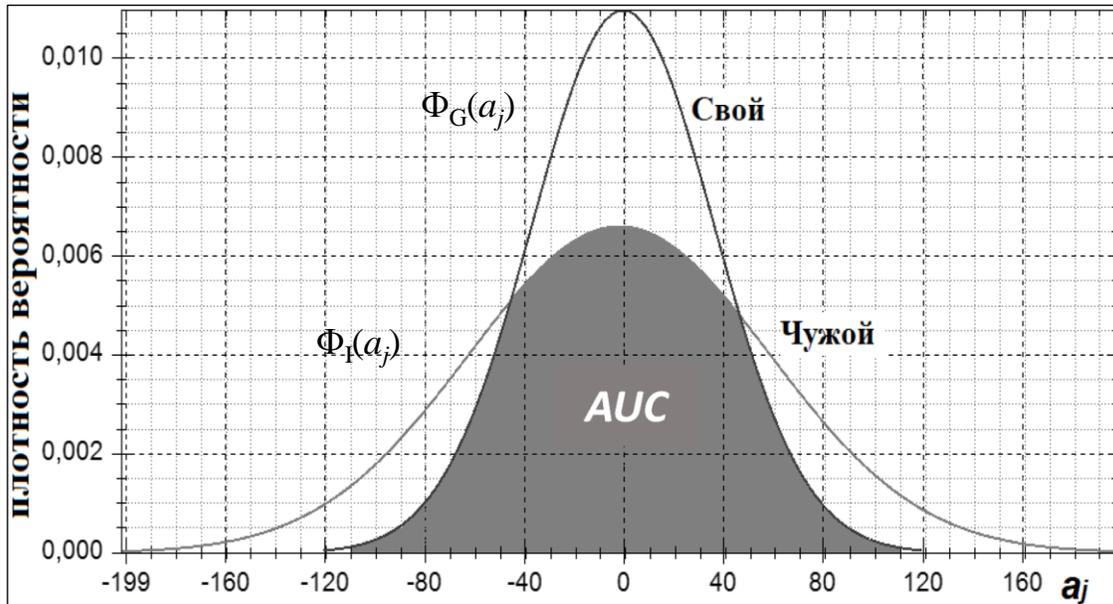


Рисунок 1 – Определение информативности признака/мета-признака для одного из классов образов

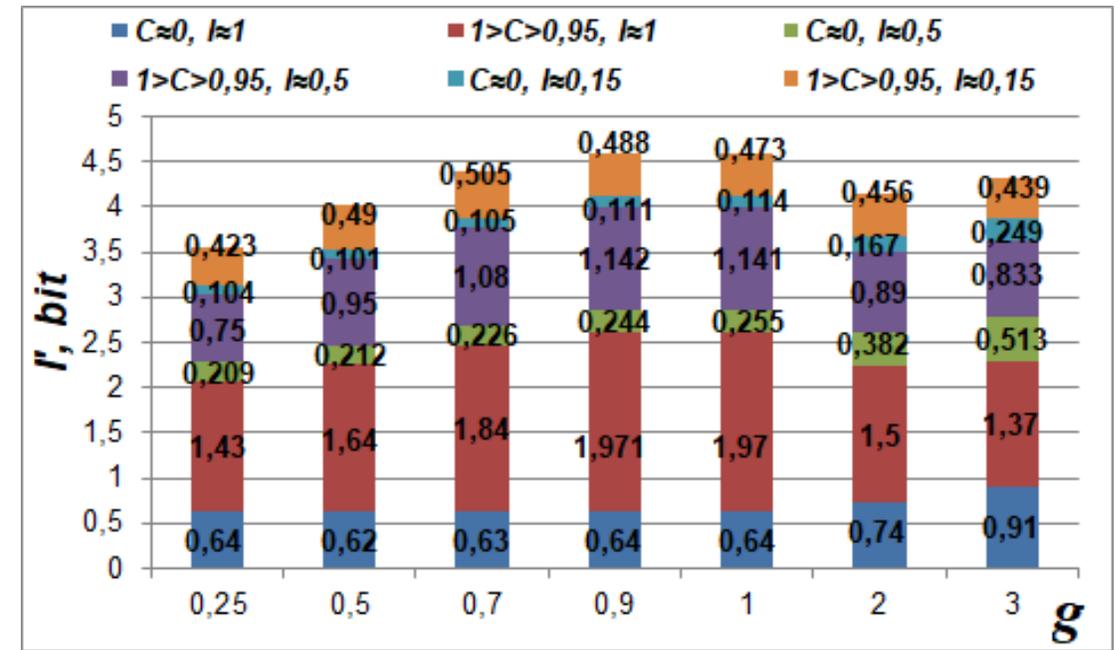


Рисунок 2 – Информативность мета-признаков \$I'\$

## Мета-признак:

$$a'_{j^*} = a'_{t,j} = f(a_t, a_j) = \left| \frac{a_t}{\delta_t} \right|^g - \left| \frac{a_j}{\delta_j} \right|^g, \quad (1)$$

$$j > t, j^* = \sum_{t^*=1}^{t-1} (n - t^*) + j - t \quad (2)$$

где  $\delta_j$  – это нормирующий коэффициент, стандартное отклонение значений признака для класса «Чужие»

## Информативность:

$$I_j = -\log_2(AUC(\Phi_G(a_j), \Phi_I(a_j))), \quad (3)$$

где  $AUC$  – площадь, ограниченная функциями плотности вероятности  $\Phi_G(a_j)$ ,  $\Phi_I(a_j)$  и осью абсцисс  $\Phi_G(a_j)$  и  $\Phi_I(a_j)$  характеризуют значения признака для классов образов («Свой») и «Чужие»

# Алгоритм синтеза и обучения корреляционного нейрона первого поколения

При настройке порогов  $T_{left}$ ,  $T_{middle}$  и  $T_{right}$  алгоритм обеспечивает:  $0,1 < P(\phi(y)) < 0,4$ , где  $P(\phi(y))$  – это относительная частота появления  $\phi(y)$  при поступлении на вход образа «Чужой»;

$\phi(y)$  – функция активации нейрона

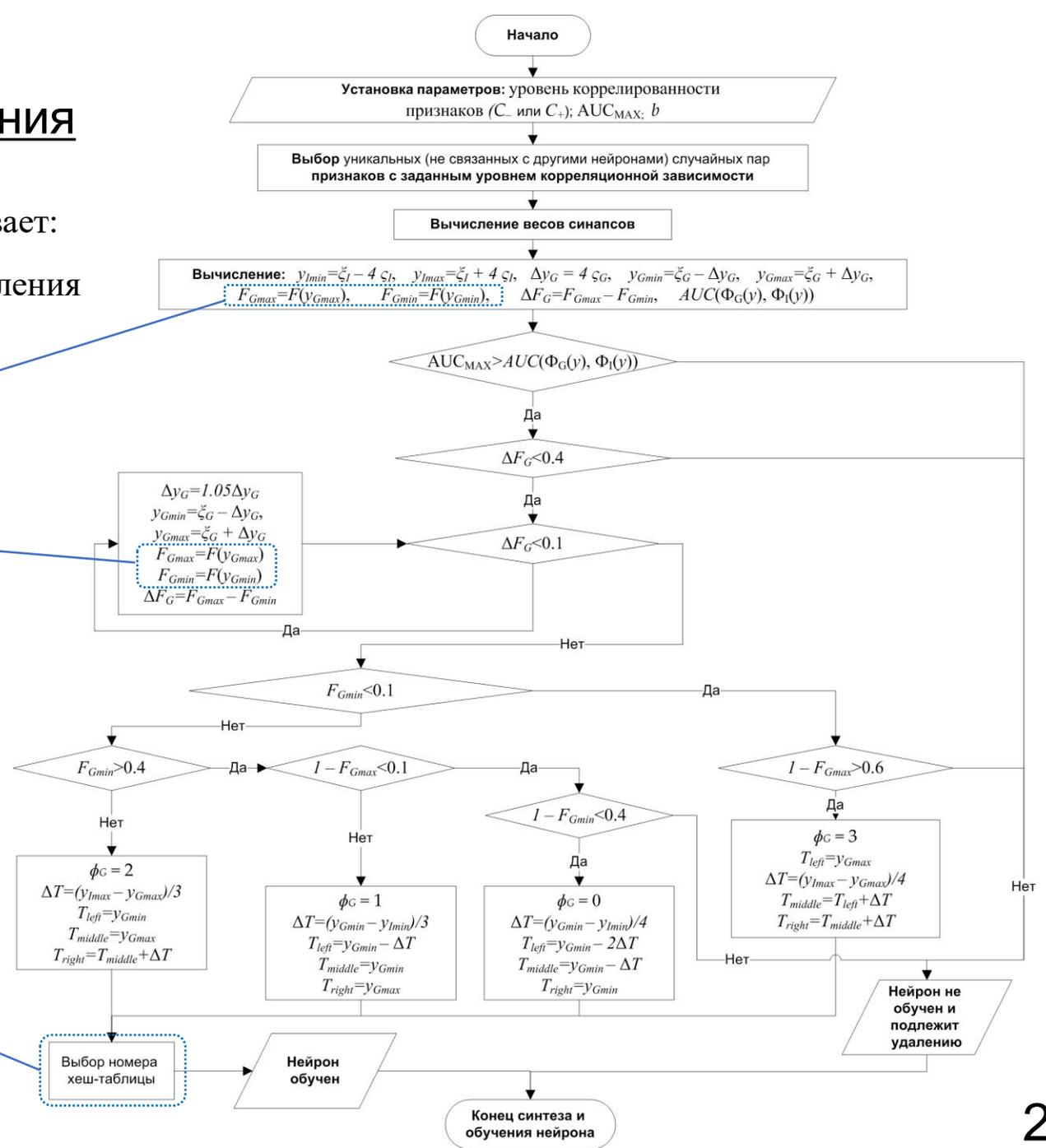
$$F(y) = \int_{-\infty}^y \frac{1}{\zeta \sqrt{2\pi}} e^{-\frac{(q-\xi)^2}{2\zeta^2}} dq,$$

$\xi$  и  $\zeta$  – математическое ожидание и стандартное отклонение  $y$  при поступлении на входы обучающих примеров

Номер преобразования  $\phi(y) \rightarrow b$  выбирается случайно, но с учетом пары **верных бит**  $b$

№ таблицы →	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(y)$ 0	«11»	«11»	«11»	«11»	«11»	«11»	«00»	«00»	«00»	«00»	«00»	«00»
1	«00»	«00»	«01»	«01»	«10»	«10»	«01»	«01»	«10»	«10»	«11»	«11»
2	«01»	«10»	«00»	«10»	«00»	«01»	«11»	«10»	«01»	«11»	«10»	«01»
3	«10»	«01»	«10»	«00»	«01»	«00»	«10»	«11»	«11»	«01»	«01»	«10»

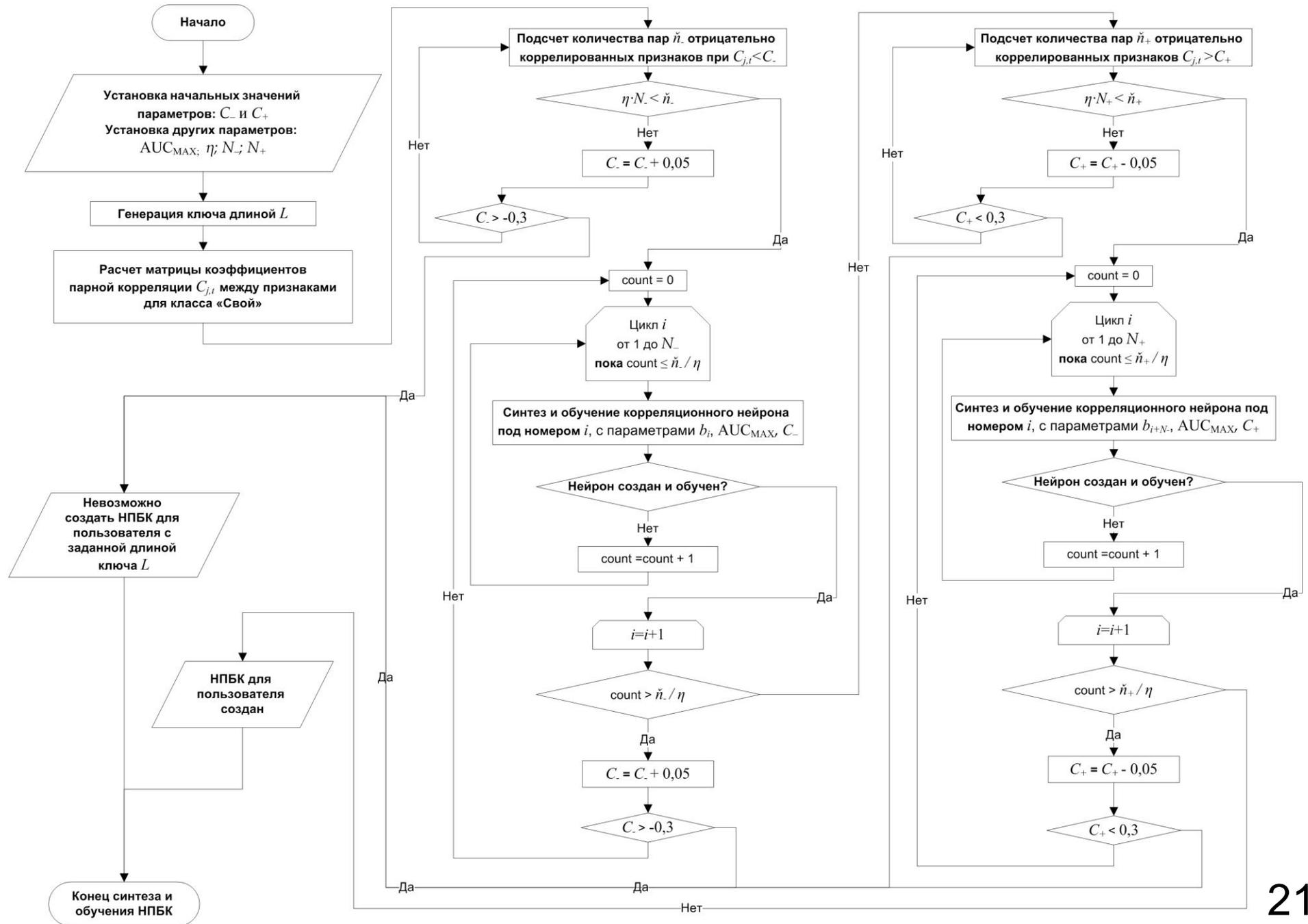
№ таблицы →	13	14	15	16	17	18	19	20	21	22	23	24
$\phi(y)$ 0	«01»	«01»	«01»	«01»	«01»	«01»	«10»	«10»	«10»	«10»	«10»	«10»
1	«00»	«00»	«10»	«10»	«11»	«11»	«00»	«00»	«01»	«01»	«11»	«11»
2	«11»	«10»	«00»	«11»	«11»	«00»	«01»	«11»	«11»	«00»	«00»	«01»
3	«10»	«11»	«11»	«00»	«00»	«10»	«11»	«01»	«00»	«11»	«01»	«00»



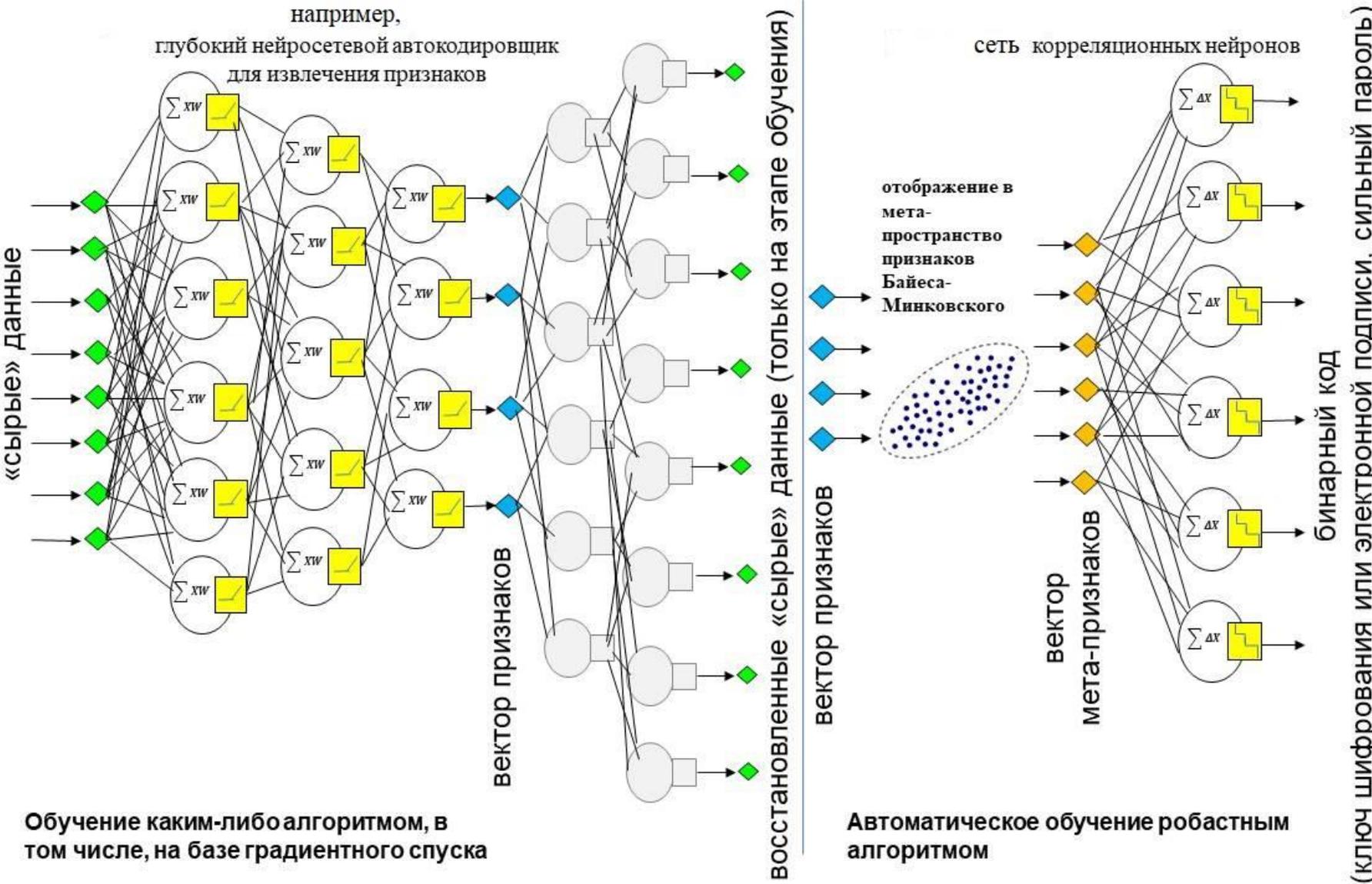
# Алгоритм автоматического синтеза и обучения НПБК

Преимущества предложенной модели НПБК и алгоритма обучения:

- полностью **автоматическое обучение** на небольших выборках
- потенциальное увеличение **длины ключа** и его энтропии за счет того, что **мета-признаков гораздо больше**
- потенциальное **снижение FRR и FAR** для слабых биометрических образов **из-за работы с корреляцией**, а не признаками
- атаки на ГОСТ Р 52633.5 более не применимы, так как **нейроны производят более одного бита** ключа



# Суть концепции защищенного исполнения нейросетевых алгоритмов ИИ



Обучение каким-либо алгоритмом, в том числе, на базе градиентного спуска

восстановленные «сырые» данные (только на этапе обучения)

Автоматическое обучение робастным алгоритмом

(ключ шифрования или электронной подписи, сильный пароль)