Сервер биометрической аутентификации: поддержка обычных и обезличенных сертификатов открытых ключей

Иванов А.И. , Безяев А.В., Корнеев О.В.

XIV PKI-Форум Россия -2016 (16 сентября, г. Санкт-Петербург)

Докладчик

Иванов Александр Иванович, д.т.н., начальник лаборатории биометрических и нейросетевых технологий АО «Пензенский научно-исследовательский электротехнический институт»

Проблема корпоративного электронного документооборота

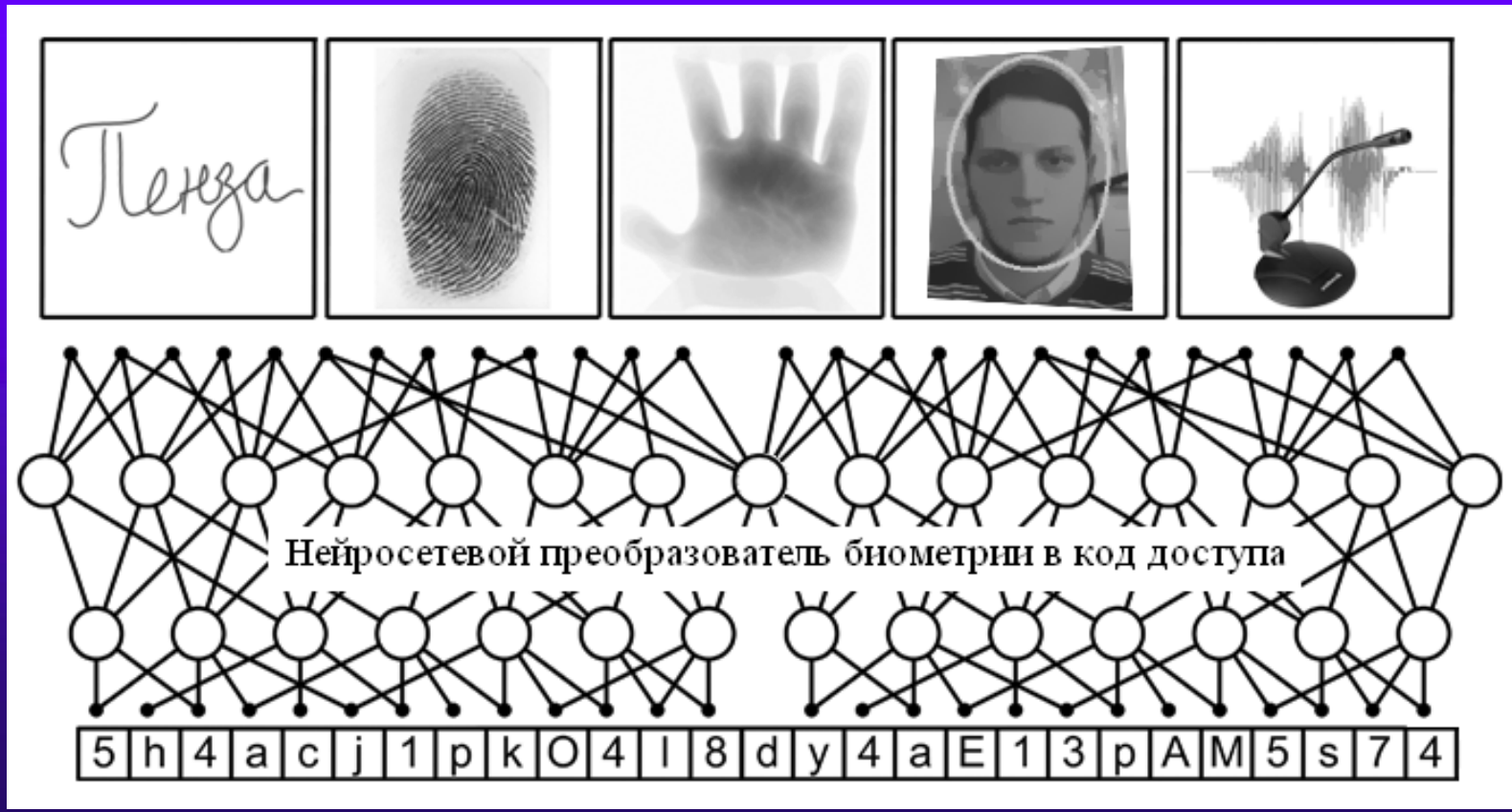
- 1. Служащие имеют возможность обмениваться токенами и паролями доступа к средству формирования ЭП
- 2. Администрация не может установить факт передачи полномочий формирования ЭП под электронным документом
- 3. Служащий имеет возможность отказаться от своей ЭП под корпоративным электронным документом

Преимущества дополнительной биометрической аутентификации

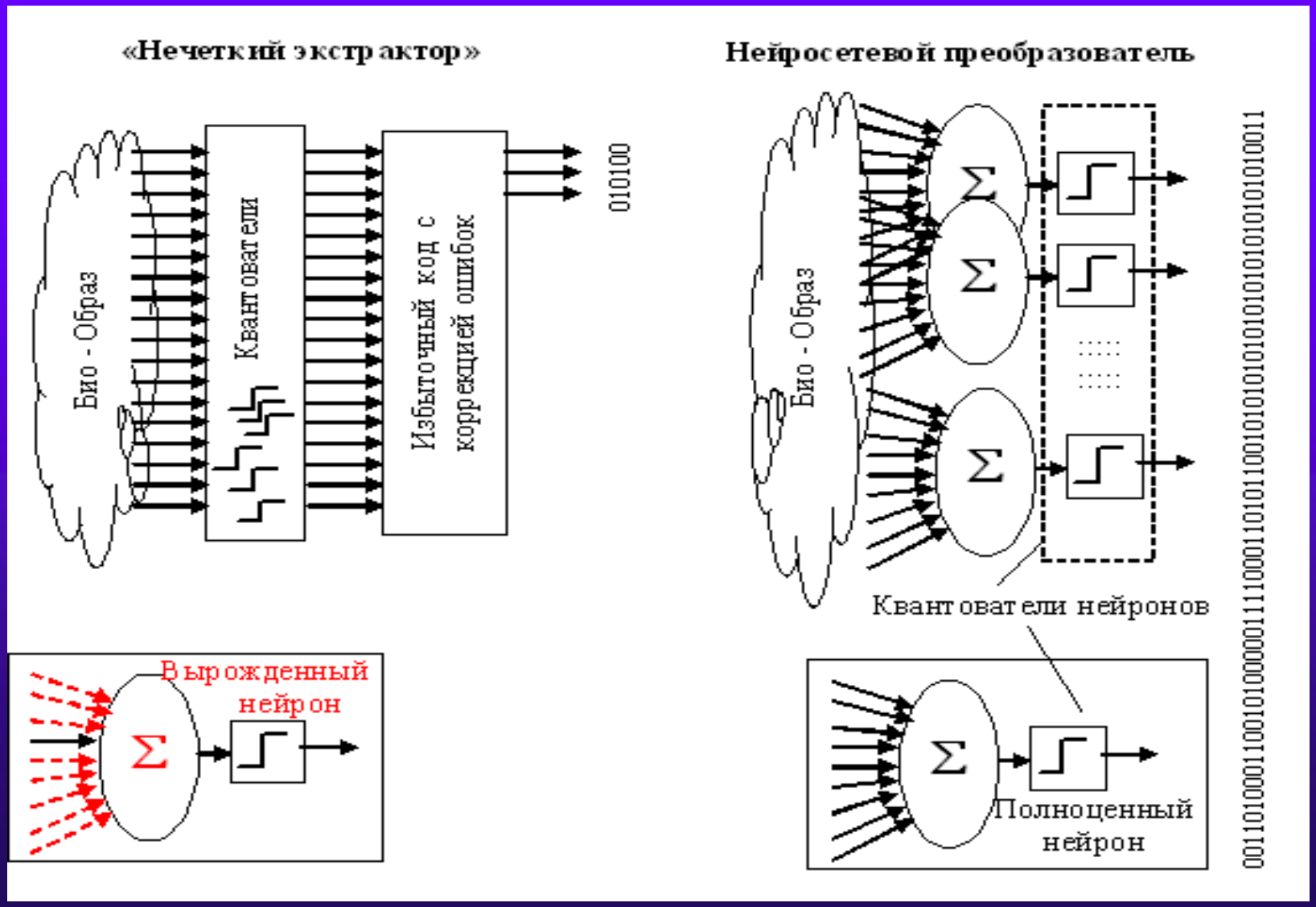
- 1. Нельзя передать свой личный ключ другому по сговору.
- 2. Нельзя отказаться от выполненных действий после биометрической аутентификации.
- 3. Чужой не может воспользоваться криптографическим ключом «соседа» из-за его халатности при использовании пароля и токена.
- 4. Нет необходимости запоминать длинные пароли из случайных символов.
- 5. Злоумышленник оставляет биометрические улики (свою биометрию) при попытках доступа.

Возможность использования мультибиометрии

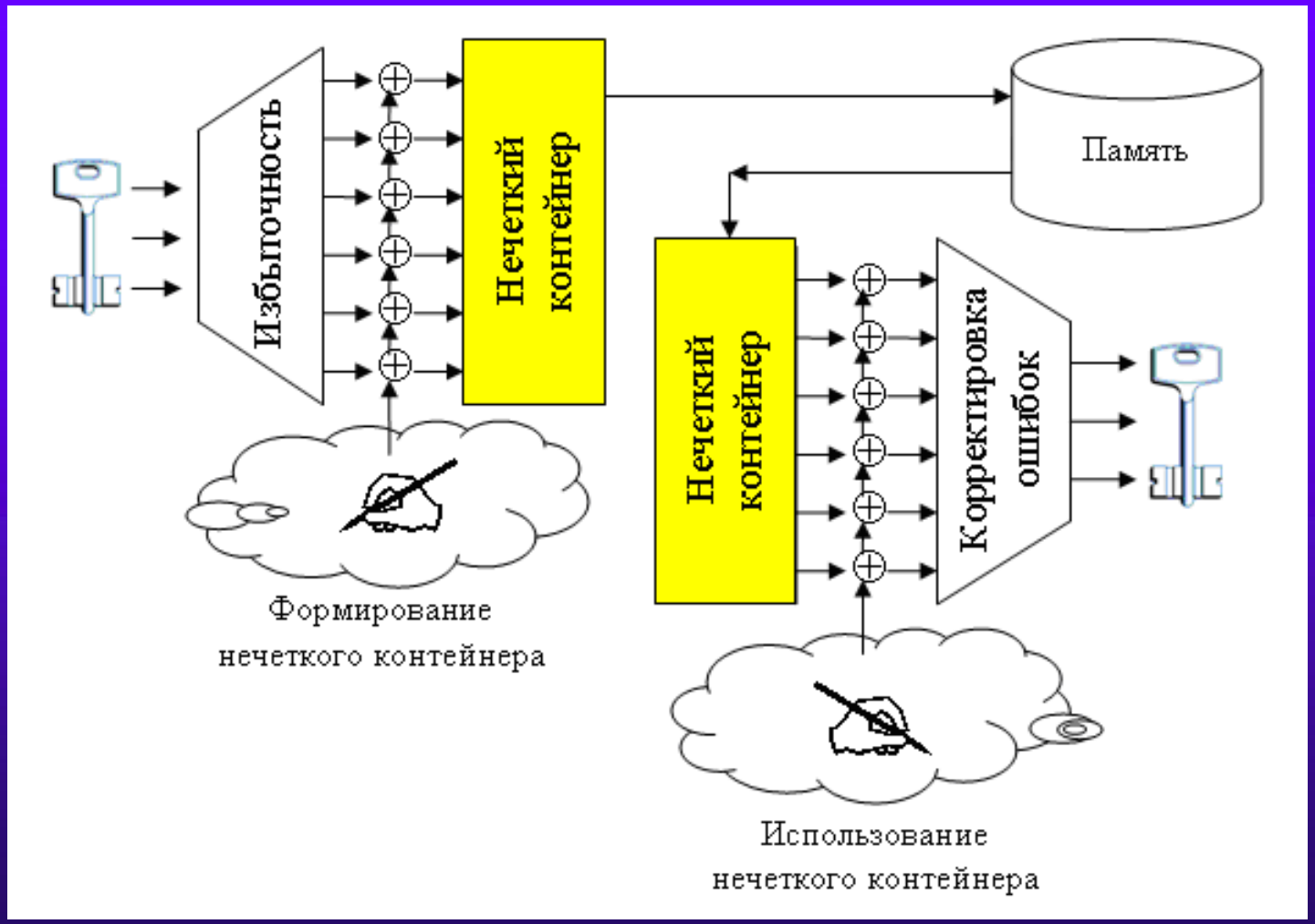
(объединение нескольких биометрических образов)



Структурные схемы «нечеткого экстрактора» и нейросетевого преобразователя биометрия-код



Технология защиты биометрических данных с использованием «нечетких экстракторов»



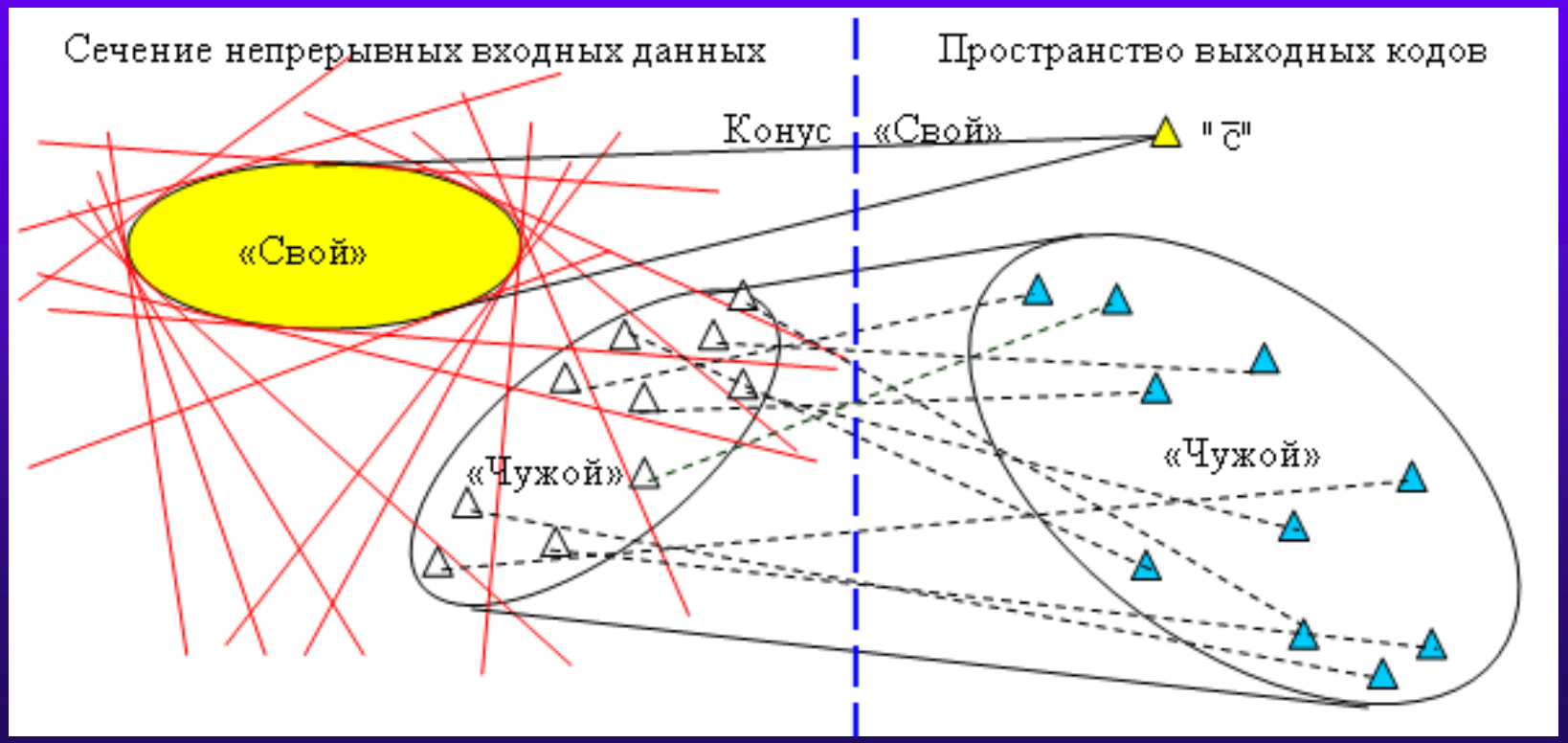
Работа нейросетевого преобразователя непрерывных многомерных континуумов биометрических данных в код ключа доступа

$$H(\nu_1, \nu_2, \ldots, \nu_n) \gg H(\text{"}c_1, c_2, \ldots, c_n\text{"}) \approx 0$$

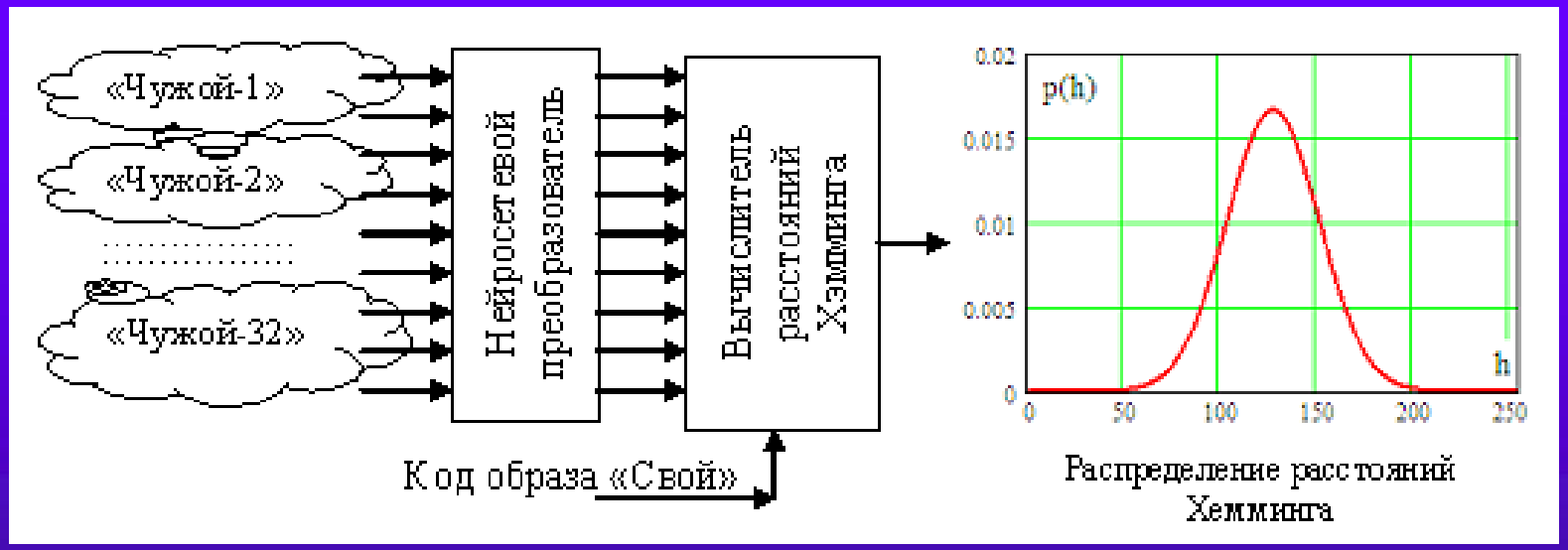
Энтропия БиоОбраза "Свой"

Энтропия БиоОбраза "Чужой"

$$H(\xi_1, \xi_2, \ldots, \xi_N) \ll H(\text{"}x_1, x_2, \ldots, x_n\text{"}) \approx \frac{n}{10}$$



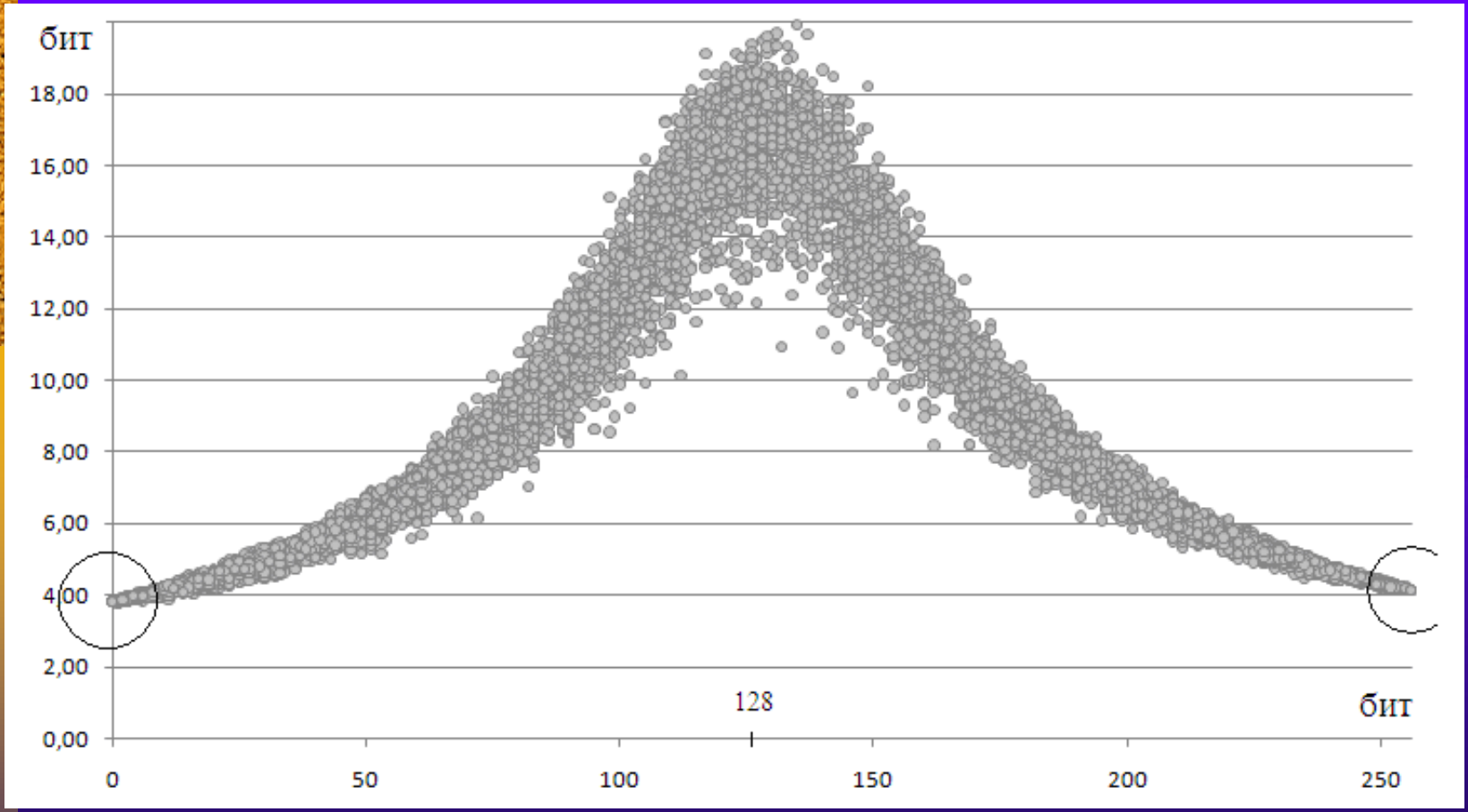
Определение энтропии выходных кодов биометрических преобразователей в пространстве расстояний Хэмминга



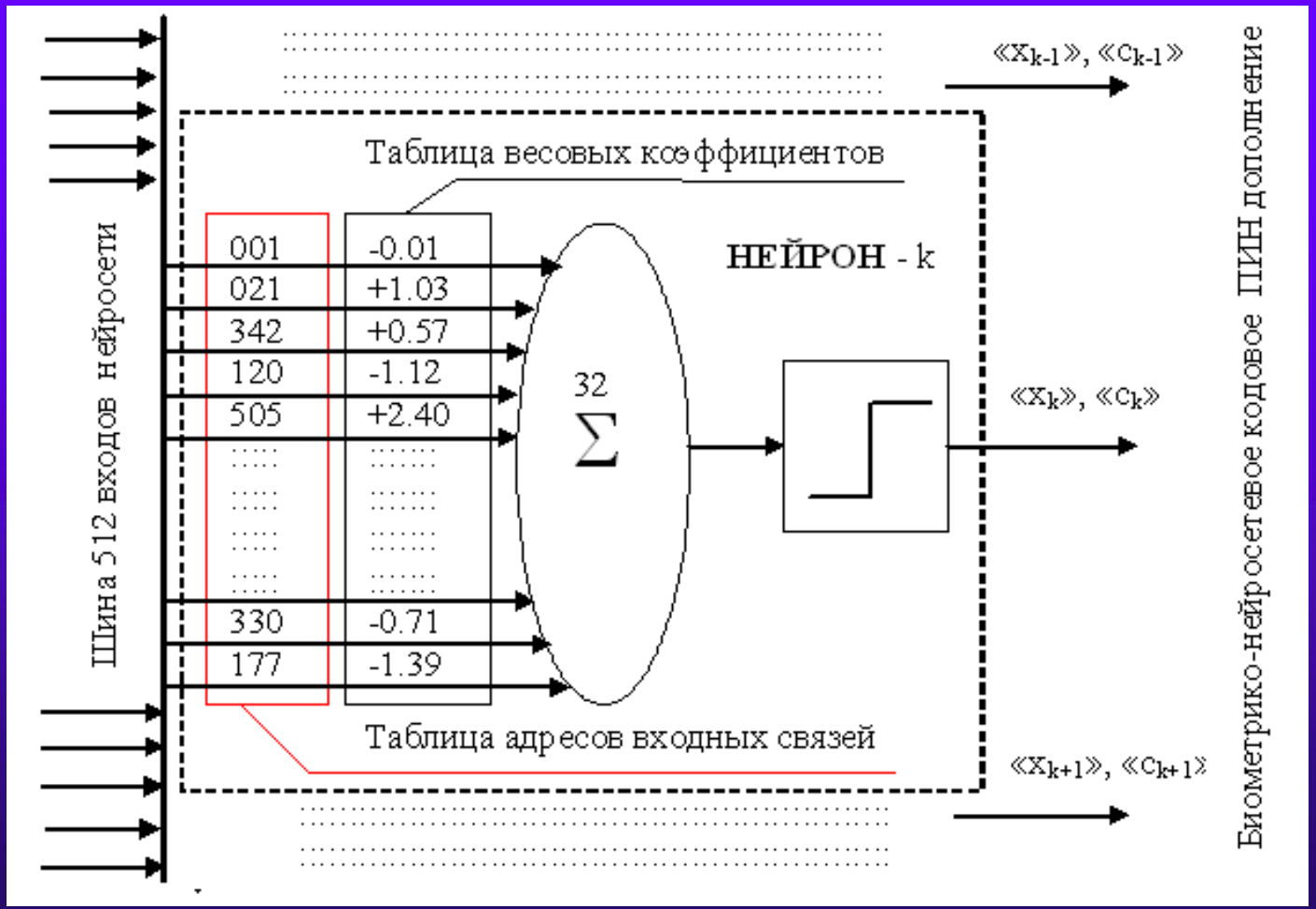
$$P_2(h_1) \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \int_{-\infty}^{h} \exp\left\{\frac{-(E(h)-u)^2}{2(\sigma(h))^2}\right\} \cdot du$$

$$H("x_1, x_2, \ldots, x_{256}") \approx -\log_2(P_2(h_1))$$

Распределение значений энтропии биометрических образов «Чужой-k» для базы из 1024 биометрических образов



Структура открытого нейросетевого контейнера с заранее сформированными таблицами связей и весовых коэффициентов



Защита нейросетевого контейнера синтезом таблиц связей каждого нейрона через рекуррентное хеширование соли, пароля и части био-кода «Свой»

$$
\begin{cases}
"a_{1,i}" = hash\{соль, пароль, i\}, \\
"a_{2,i}" = hash\{соль, пароль, c_1, i\}, \\
\quad \ldots\ldots\ldots \quad \ldots\ldots\ldots \quad \ldots\ldots\ldots \quad \ldots\ldots\ldots \quad \ldots\ldots \\
"a_{k,i}" = hash\{соль, пароль, c_1, c_2, \ldots, c_{k-1}, i\}
\end{cases}
$$

Состояния разрядов кода "Свой"

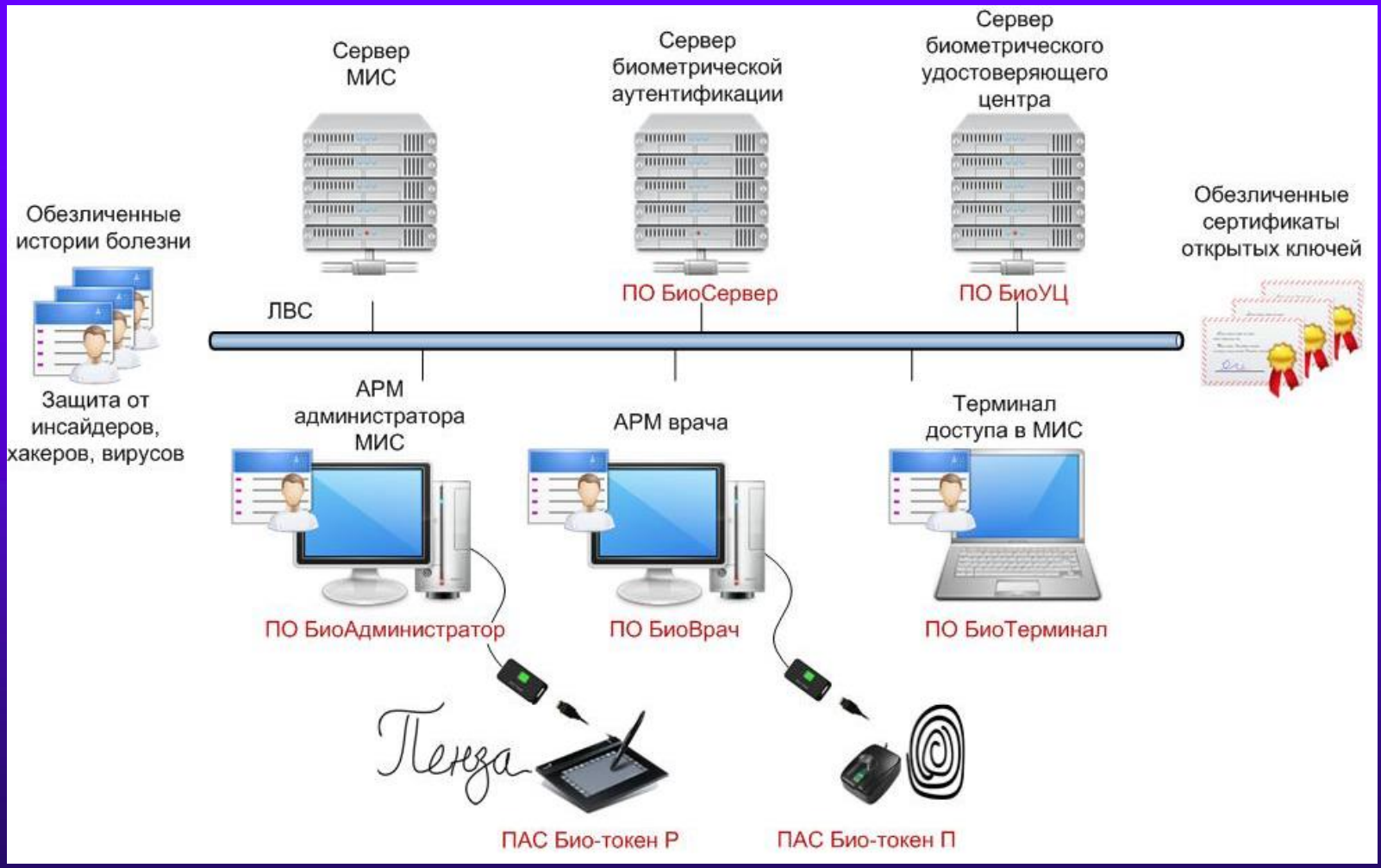
$i = 1, 2, \ldots, 32$; Номер входа нейрона

$k = 1, 2, \ldots\ldots, 256$ Номер нейрона

Гарантии безопасности биометрии:

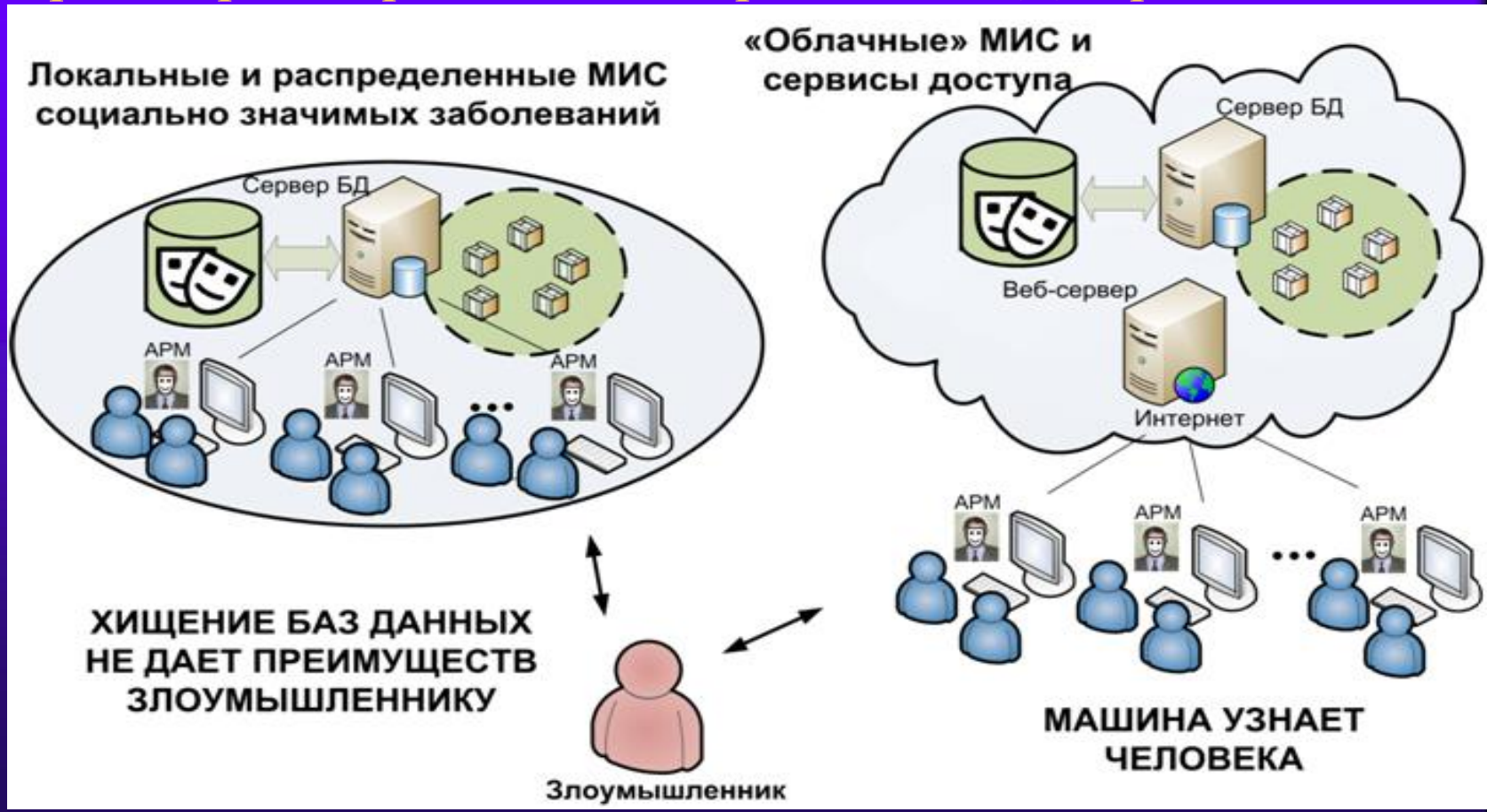
1. Открытая биометрия, распакованные нейронные сети, личный ключ формирования ЭП не покидают доверенной вычислительной среды USB БиоТокен, включаемой между сканером биометрии и ПЭВМ;
2. Биометрия на сервере биометрической аутентификации хранится в защищенном нейросетевом контейнере (хранится программа вызова функций хеширования, восстанавливающая таблицы связей обученной нейронной сети).

Структура медицинской информационной системы, поддерживающей обезличенные электронные документы (обезличенные сертификаты открытых ключей)



Причины по которым приходится обезличивать сертификаты открытых ключей:

1. открытое локальное хранение электронных историй болезни в МИС;
2. использование «облачных» сервисов для хранения, транспорта, обработки электронных МЕД-карт.



Доклад окончен.

Спасибо за внимание!