АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРА НА ОСНОВЕ КЛАВИАТУРНОГО ПОЧЕРКА И ОСОБЕННОСТЕЙ ЛИЦА[1]

Ложников П.С.[2], Сулавко А.Е.[3], Бурая Е.В.[4], Писаренко В.Ю.[5]

Рассмотрена проблема распознавания пользователя в процессе работы на компьютере в пространстве признаков клавиатурного почерка и лица. Предложено несколько подходов к формированию решений: сети персептронов, сети Пирсона–Хемминга, Байеса–Пирсона–Хемминга, Байеса–Хемминга. Подтверждено, что многомерный функционал Байеса работает тем лучше, чем выше коэффициент равной коррелированности признаков и выше его размерность. Показано, что для различных признаков могут быть найдены функционалы, наилучшим образом работающие с ними. Установлено, что при увеличении времени мониторинга пользователя удается существенно снизить ошибочные решения за счет более точного вычисления значений признаков. Предложен способ генерации ключей, которые можно использовать для шифрования, формирования ЭЦП или аутентификации с вероятностями ошибочных решений, зависящими от времени мониторинга действий субъекта при активной его работе на компьютере: 30 секунд – FRR=0,002, FAR=0,0036; 60 секунд – FRR=0,002, FAR=0,0009; 150 секунд – FRR<0,0005, FAR<0,0005.

***Ключевые слова**: распознавание субъектов, биометрический признак, длительность мониторинга, генерация ключей, шифрование, электронная цифровая подпись*

DOI: 10.21681/2311-3456-2017-3-24-34

Введение.

На сегодняшний день функционирование большинства предприятий сложно представить без использования программного обеспечения (ПО), которое применяется для разных целей: проведения финансовых транзакций, создания продуктов, документов, оказания услуг и др. Вопросы защиты ПО и создаваемого при помощи него контента являются крайне важными. Возрастает потребность в разработке и приобретении эффективных систем непрерывного мониторинга и аутентификации пользователей ПО в режиме реального времени. По данным PricewaterhouseCoopers (PwC) на октябрь 2016 года 62% руководителей предприятий используют системы аутентификации и мониторинга работников, 57% используют биометрическую аутентификацию [1].

Заинтересованность России в развитии рынков систем информационной безопасности, в том числе биометрических, находит отражение в структуре НТИ (Национальной технологической инициативы – долгосрочной комплексной программе по созданию условий для обеспечения лидерства российских компаний на новых высокотехнологичных рынках, которые будут определять структуру мировой экономики в ближайшие 15–20 лет). В проекте НТИ выделяется рынок безопасных и защищенных компьютерных технологий, решений в области передачи данных, безопасности информационных и киберфизических систем (SafeNet), целый сегмент которого (Прикладные системы для решения задач безопасности) практически полностью посвящен решению задач, связанных с биометрией: внедрению впервые в мире национальной биометрической платформы аутентификации, ЭЦП с биометрической активацией и тому подобных.

Сегодня при выполнении Internet-операций купли-продажи или при формировании ЭЦП используются криптографические ключи, которые являются отчуждаемыми от владельца и могут быть переданы третьим лицам. По этой причи-

1 Работа выполнена при финансовой поддержке РФФИ грант №16-37-50049

2 Ложников Павел Сергеевич, к.т.н., доцент, ФГБОУ ВО Омский государственный технический университет (ОмГТУ), г. Омск, Россия. E-mail: lozhnikov@gmail.com

3 Сулавко Алексей Евгеньевич, к.т.н., ФГБОУ ВО Омский государственный технический университет (ОмГТУ), г. Омск, Россия. E-mail: sulavich@mail.ru

4 Бурая Екатерина Викторовна, ФГБОУ ВО Уфимский государственный авиационный технический университет (УГАТУ), г. Уфа, Россия. E-mail: burka-777@yandex.ru

5 Писаренко Виктор Юрьевич, ФГБОУ ВО Омский государственный технический университет (ОмГТУ), г. Омск, Россия. E-mail: j-e-d-y@mail.ru

не ключ можно забыть, потерять, подменить, украсть. Решить описанные проблемы можно, если связать все аутентификаторы субъекта (паролей, ключей шифрования, кодов доступа и т.д.) с его биометрическим характеристикам достаточно надежным способом. Процедура ввода биометрических характеристик должна быть ненавязчивой, не должна нарушать или усложнять существующие бизнес-процессы в организации, внедрение новых методов защиты документов должно быть экономически обоснованным. Биометрический образ субъекта должен быть тайным либо его копирование или воспроизведение другими лицами на практике должно быть неосуществимым. Плюсом в сложившейся ситуации будет являться возможность реализации средств защиты на стандартном оборудовании компьютерных систем.

Статические образы (отпечаток пальца, радужка) находятся «на виду», существует множество способов их незаметного копирования с изготовлением электронного и физического муляжа. Статические образы нельзя ввести при помощи стандартного оборудования компьютера. Для аутентификации в реальном времени при использовании стандартного оборудования подходят параметры клавиатурного почерка и лица субъекта, регистрируемые в процессе работы на компьютере [2]. Однако данные технологии на практике пока характеризуются высоким числом ошибок аутентификации субъектов. Настоящая работа направлена на повышение надежности процедуры непрерывной аутентификации в реальном времени в пространстве данных признаков.

1. Формирование данных о работе пользователя на компьютере.

В процессе исследований сформирована база биометрических образцов 100 испытуемых. Все испытуемые решали тестовые задания на компьютере, при этом осуществлялся мониторинг их действий с использованием разработанного программного модуля. Веб-камера была направлена по отношению к испытуемому таким образом, чтобы было возможно осуществить локализацию лица субъекта (пользователь был повернут лицом к камере либо с незначительным углом отклонения от нее). Тестовые задания создавали необходимость ввода текста на клавиатуре, также демонстрировались изображения, вследствие чего, субъект вынужден был смотреть на экран (в направлении камеры). Частота съемки составила 15 кадров в секунду, с разрешением видео 800x600. Длительность тестового задания составляла 1 час. Программный модуль скрыто регистрировал следующие данные:

- при обнаружении лица (и основных ключевых особенностей лица) в кадре осуществлялась видеосъемка, разложение видеоданных на последовательность кадров, содержащих только изображение лица;

- при нажатии на клавишу регистрировалось время удержания клавиш и пауза между нажатием этой и предыдущей клавиши.

Собранные данные подвергались статистической обработке, в результате из каждого образца вычислялся вектор значений признаков – величин, характеризующих испытуемых.

2. Оценка информативности признаков.

В настоящей работе использовались следующие группы признаков лица:

1. Расстояния между глазами, правым (левым) глазом и центром лица, правым (левым) глазом и кончиком носа, правым (левым) глазом и центром рта, центром рта и центром лица, кончиком носа и центром рта, центром рта и кончиком носа (в пикселях, значения нормировались по диагонали лица в кадре).

2. Площади глаз, носа, рта (значения нормировались по площади лица).

3. Коэффициенты корреляции яркости и цветовых составляющих пикселей (в соответствии с моделью RGB) между всеми парами следующих областей лица: правый глаз, левый глаз, нос, рот. Данные признаки характеризуют мимику, асимметрию и непроизвольные движения лица субъектов.

4. Коэффициенты корреляции яркости и цветовых составляющих пикселей (в соответствии с моделью RGB) следующих областей лица, выделяемых на соседних кадрах: правый глаз, левый глаз, нос, рот. Данные признаки характеризуют мимику и непроизвольные движения лица.

5. Средние показатели интенсивности яркости, а также красной (R), зелёной (G) и синей (B) составляющих пикселей, характеризующих цвет глаз и кожи.

Для выделения лица, глаз, носа, рта использовался метод Виолы-Джонса, позволяющий детектировать объекты на изображениях в реальном времени [3]. Данный метод распознавания объектов на изображении является одним из лучших по эффективности распознавания и скорости работы

(обладает крайне низкой вероятностью ошибок и распознает черты лица под углом до 30 градусов) [4-5]. Для разделения области радужки и зрачка производится поиск внутренней границы радужки (внешней границы зрачка) при помощи алгоритма обнаружения окружностей на основе преобразования Хафа [6].

Имеется погрешность вычисления описанных 62 признаков, связанная с точностью работы метода Виолы-Джонса и преобразования Хафа, условиями съемки и особенностями видеозаписей. Все признаки имеют распределение, достаточно близкое к нормальному, что проверялось критерием Хи-квадрат.

Признаками клавиатурного почерка являются временные интервалы между нажатием клавиш и длительности их удержания. Известно, что значения данных характеристик имеют распределение близкое к нормальному [7].

Информативность признаков определяется площадями пересечения между всеми парами функций плотностей вероятности (рис. 1) каждого признака, характеризующими испытуемых. Также важным фактором является взаимная корреляционная зависимость признаков (рис 2).

Также в качестве признаков рассматривались особенности траекторий перемещения курсора мыши из работы [8]. Однако площади пересечения плотностей вероятности для данных признаков оказались слишком значительны (более 80% площадей превысило 0,7) и от данных признаков решено отказаться.

3. Нечеткие экстракторы.

В настоящее время популярен подход к решению рассматриваемых задач, называемый «нечетким экстрактором» [9], основанный на использовании классических кодов, исправляющих ошибки генерируемого ключа, применяемых к не обогащенным векторам значений признаков после их предварительного квантования. Метод исправляет ошибки, возникающие вследствие невозможности получения одинаковых биометрических образов при их повторном воспроизведении. К принципиальным недостаткам подхода относятся [10]:

1. Длина генерируемого ключа оказывается низкой из-за избыточности классических самокорректирующих кодов (чем больше ошибок исправляет код, тем короче итоговый ключ) [11]. Для решения проблемы в [12] предложены коды, раз-

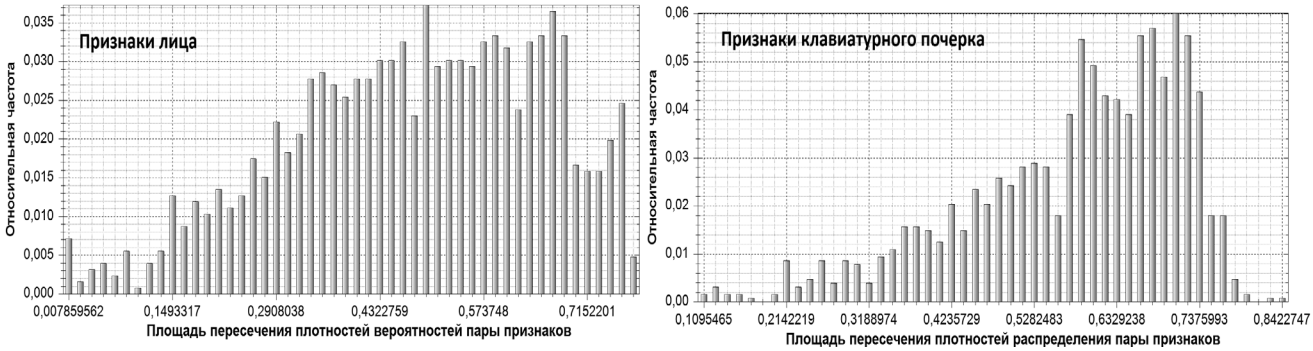

***Рис.1**. Площади пересечения всех пар функций плотностей вероятности каждого признака, характеризующих различных испытуемых*

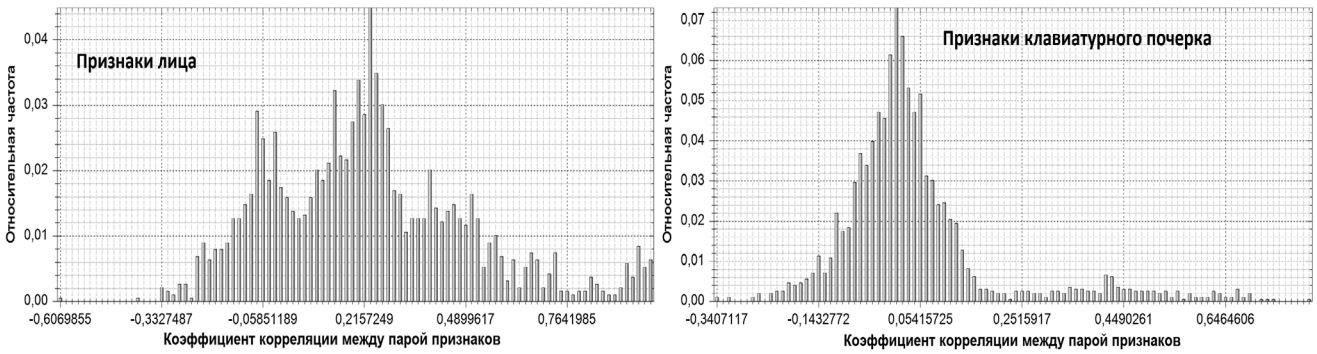

***Рис.2**. Коэффициенты корреляции между всеми парами сечений признаков*

работанные специально для биометрии. Они позволяют хранить синдромы ошибок отдельно от открытой строки в виде усеченной хеш-функции, поэтому извлекаемый из открытой строки ключ доступа будет значительно длинней.

2. В [13] описаны уязвимости нечетких экстракторов, позволяющие ускорить перебор значений биометрических параметров с целью фальсификации ключа доступа. Наложение на биометрические данные гаммы в виде строки бит является надежной защитой для обеих составляющих только в случае равновероятной единичной ошибки в битовом представлении вектора значений признаков, чего на практике не наблюдается [13]. Несмотря на предпринятые усилия [14], единого подхода для решения проблемы не выработано.

3. Нечеткие экстракторы квантуют биометрические данные без предварительного обогащения, не учитывая параметры распределения значений признаков [11, 13]. Поэтому данные признаки способны работать только с очень информативными признаками (с площадями пересечения функций плотностей вероятности признаков порядка 0 – 0,3). Данная проблема не имеет решения.

В работе [10] проведено экспериментальное сравнение нечетких экстракторов и нейросетевых преобразователей биометрия-код – в задаче генерации ключей из подписей субъектов нечеткие экстракторы оказались малоэффективны. В силу изложенных причин от нечетких экстракторов решено отказаться.

4. Нейросетевой подход к генерации ключа и последующей аутентификации субъектов.

Рекомендуемым подходом в России является использование искусственных нейронных сетей на основе персептронов, обучаемых по ГОСТ Р 52633.5-2011. Алгоритм из ГОСТ Р 52633.5 служит для послойного детерминированного обучения сети нейронов: сначала осуществляется обучение первого слоя, далее эти же обучающие данные подаются на вход второго слоя сети. Рекомендуется использовать только однослойные или двухслойные сети персептронов (первый слой обогащает данные, второй играет роль кодов, исправляющих ошибки [11]). Алгоритм обучения позволяет настроить сеть на выдачу определенного пользователем ключа при поступлении образа этого пользователя (образа «Свой») и случайной слабокоррелирующей битовой последовательности (близкой к белому шуму) при поступлении образа неизвестного пользователя (образа «Чужой»). Для каждого субъекта создается своя сеть, которая работает в режиме верификации образов. Для обучения требуется не менее 21 образца «Свой» и 64 образцов «Чужой». В процессе обучения вычисляются весовые коэффициенты нейронов, исходя из параметров законов распределения значений признаков для образов «Свой» и «Чужой»: среднеквадратичных отклонений и математических ожиданий, после обучения эти данные удаляются, чтобы избежать компрометации биометрического эталона и ключа [11].

Обучение сети нейронов стандартным алгоритмом обладает рекордной устойчивостью и имеет линейную вычислительную сложность, так как в нем исключен направленный итерационный поиск весовых коэффициентов нейронов.

Обогащение данных персептронами не является оптимальным. Существует множество функционалов, обогащающих данные более эффективно. Одним из них является классическая квадратичная форма (1):

$$y(\bar{v}) = (E(\bar{v}) - \bar{v})^T \cdot [R]^{-1} \cdot (E(\bar{v}) - \bar{v}), \quad (1)$$

где $\bar{v}$ – вектор нормированных биометрических параметров с единичными стандартными отклонениями, $[R]^{-1}$ – обратная корреляционная матрица признаков (матрица коэффициентов парной корреляции между сечениями признаков). Для биометрических параметров обращение корреляционных матриц высоких порядков (более 5) невозможно – возникает эффект «проклятия» размерности. В связи с этим часто используются сети из квадратичных форм, не учитывающих корреляционные связи. Самой распространенной является метрика хи-квадрат Пирсона (2):

$$\chi = \sum_{i=1}^{m} \frac{(E(v_i) - v_i)^2}{\sigma(v_i)^2}, \quad (2)$$

где v_i – значение i-ого признака (входа нейрона), $E(v_i)$ – мат. ожидание (среднее значение) i-ого признака (входа нейрона), $\sigma(v_i)$ – среднеквадратичное отклонение i-ого признака (входа нейрона). Мощность метрики Пирсона (2) падает при ее применении к зависимым данным (более 0,3) [15]. В качестве альтернативы может быть использована метрика Байеса-Пирсона (3) [16]:

$$\chi = \sum_{j=1}^{m} \sum_{i=1}^{m} \left| \frac{|E(v_i) - v_i|}{\sigma(v_i)} - \frac{|E(v_j) - v_j|}{\sigma(v_j)} \right|, \quad (3)$$

где v_i – значение i-ого признака (входа нейрона), $E(v_i)$ – мат. ожидание i-ого признака (входа нейро-

на), $\sigma(v_i)$ – среднеквадратичное отклонение i-ого признака (входа нейрона). Метрика Байеса-Пирсона (3) как и метрика Пирсона (2) не содержит вычислительных операций с коэффициентами корреляции, но сильно зависит них.

В работе [17] предложено использовать многомерные Байесовские функционалы [17] (4), ориентированные на использование только сильно коррелирующих признаков:

$$y_{k,j} = \sum_{i=1}^{m} \left| \frac{|M(a_k) - a_{k,j}|}{\sigma(a_k)} - \frac{|M(a_i) - a_{i,j}|}{\sigma(a_i)} \right| , \quad (4)$$

где $a_{i,j}$ – значение i-ого признака (входа нейрона) с высоким значением модуля корреляции $|r_{i,k}|$ по отношению к k-ому биометрическому признаку $a_{k,j}$ $(i \neq k)$, j – номер биометрического образца образа «Свой», для которого вычисляется функционал, $M(a_i)$ и $\sigma(a_i)$ – математическое ожидание и среднеквадратичное отклонение i-ого признака (входа нейрона). Нетрудно убедиться, что при функциональной зависимости признаков значение метрики (4) будет иметь нулевое значение для любого образца «Свой». По мере снижения коэффициентов корреляции значение функционала (4) возрастает, растет также его стандартное отклонение. Исследования показывают, что многомерный функционал Байеса работает тем лучше, чем выше коэффициент равной коррелированности признаков и выше его размерность. Под равной коррелированностью подразумевается, что разница модуля коэффициентов корреляции не превышает τ.

Независимо от типа нейрона значение на выходе его функционала сравнивается с пороговым. Для каждого нейрона существует оптимальный порог срабатывания, который вычисляется (кроме персептронов, для которых процесс настройки полностью определяется стандартом) исходя из откликов обучающих примеров образа «Свой» [10]. Если порог превышен, нейрон выдает единицу («1»), иначе нуль («0»). Настройка сети на нужный выходной код производится инвертированием выходных значений отдельных нейронов. Так как нейроны выдают бинарные значения, их сети называют по имени метрики и Хемминга.

5. Оценка эффективности генерации ключа с использованием сетей из различных функционалов.

Проведен вычислительный эксперимент. Биометрические образы были преобразованы в векторы биометрических параметров (реализации). Для обучения использовалось по 21 реализации образа «Свой» (а также по 1 реализации каждого образа для обучения персептронов на данных «Чужой»). Далее проводились серии опытов по верификации субъектов сетями персептронов, Байеса-Пирсона-Хемминга, Пирсона-Хемминга и Байеса-Хемминга. Если генерируется нехарактерный для субъекта ключ, происходит ошибка 1-ого рода. За ошибку 2-ого рода принимается ситуация, при которой ключ, полученный из биометрических данных субъекта, соответствует или близок к ключу другого субъекта. Вероятности ошибок 1-ого (FRR, false reject rate) и 2-ого (FAR, false acceptance rate) рода характеризуют надежность методики генерации ключа. При верификации ключа решение принимается исходя из расстояния Хемминга H между генерируемым и верным битовыми последовательностями. После выработки ключа сетью ($H=0$) производилась корректировка его ошибочных бит при помощи кодов из работы [12] ($H>0$). В процессе эксперимента изменялись значения параметров N, m, τ и ϕ – максимальный модуль коэффициента корреляции между признаками, менее которого признаки не учитывались сетью Байеса-Хемминга. Эксперимент повторялся в 3-х вариантах: на входы сетей подавались векторы значений признаков, вычисляемые по данным мониторинга длительностью 30, 60 и 150 секунд. При этом предварительно вы числялись средние значения дублирующихся признаков. Это позволяет обеспечить повышение стабильности значения признака – снизить среднеквадратичное отклонение (рис. 3). За счет этого при увеличении длительности мониторинга и накоплении большего количества значений признаков удается добиться снижения числа ошибок (табл. 1). Подсчитывалось общее число ошибок 1-ого и 2-ого рода, FRR и FAR вычислялись как отношения количества ошибок соответствующего рода к числу проведенных опытов с использованием реализаций «Свой» или «Чужой». Далее приведены графики вероятностей ошибки верификации испытуемых за время мониторинга 30 секунд при оптимальных значениях порога (определяется по минимуму FRR+FAR в каждой серии испытаний) после корректировки кодами [12] (рис. 4-6). Дополнительная корректировка ошибок в ключе позволяет достичь существенно более низкой суммы вероятностей ошибок 1-ого и 2-ого рода.

Таблица 1.
Наилучшие результаты эксперимента (КП – клавиатурный почерк).

Признаки	Время мониторинга	Тип сети	Параметры сети	FRR	FAR
Лицо	30 секунд	Пирсона-Хемминга	N=50, m=5	0,0014	0,002
КП	30 секунд	Персептроны	N=80, m=10	0,058	0,0636
Лицо + КП	30 секунд	Байеса-Пирсона-Хемминга	N=120, m=5	0,002	0,0036
Лицо	60 секунд	Пирсона-Хемминга	N=80, m=15	≈0	0,0002
КП	60 секунд	Персептроны	N=200, m=50	0,034	0,043
Лицо + КП	60 секунд	Персептроны	N=60, m=25	0,002	0,0009
Лицо	150 секунд	Любой	Различные	≈0	≈0
КП	150 секунд	Любой (кроме персептронов)	Различные	≈0	≈0
Лицо + КП	150 секунд	Любой	Различные	≈0	≈0

Наилучший результат в разных случаях достигается различными сетями. Сеть Байеса-Хемминга не дает наилучших результатов, из-за малого количества сильно коррелирующих признаков (рис. 2). При поступлении в сеть Байеса-Хемминга слабо коррелирующих признаков совместно с сильно коррелирующими вероятности FRR и FAR становятся выше, т.е. многомерный функционал Байеса работает тем лучше, чем сильней корреляция между признаками.

Выводы

Сформирована база биометрических образов лица и клавиатурного почерка 100 испытуемых в процессе их длительного (30 минут) непрерывного мониторинга при работе на компьютере. Проведен эксперимент по распознаванию образов субъектов при различном времени мониторинга: 30, 60 и 150 секунд (синтезированы усредненные естественные биометрические образы, количество тестовых образцов каждого вида составило соответственно 12000, 6000 и 2400). С увеличением времени мониторинга удается существенно снизить количество ошибочных решений. При времени мониторинга 150 секунд вероятность ошибок снижается практически до нуля при использовании признаков лица и клавиатурного почерка, как в отдельности, так и совместно. При комплексировании 2-х независимых образов резко усложняется возможность фальсификации системы. Вероятности ошибок составили:

30 секунд – FRR=0,002, FAR=0,0036;
60 секунд – FRR=0,002, FAR=0,0009;
150 секунд – FRR<0,0005, FAR<0,0005.

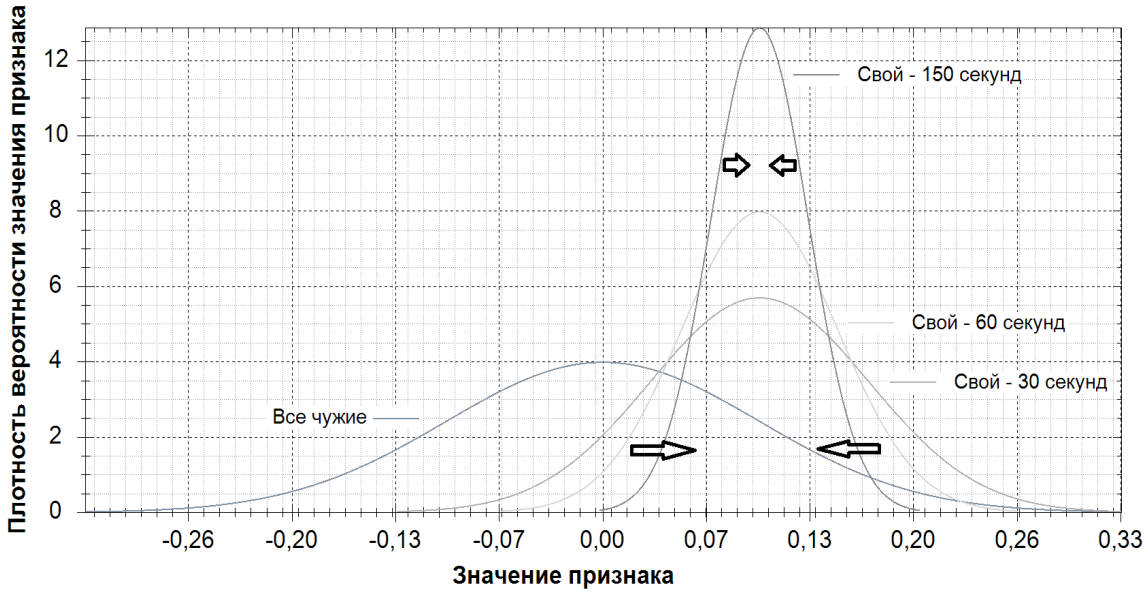

***Рис.3**. Уменьшение среднеквадратичного отклонения средних значений признаков при увеличении времени мониторинга.*

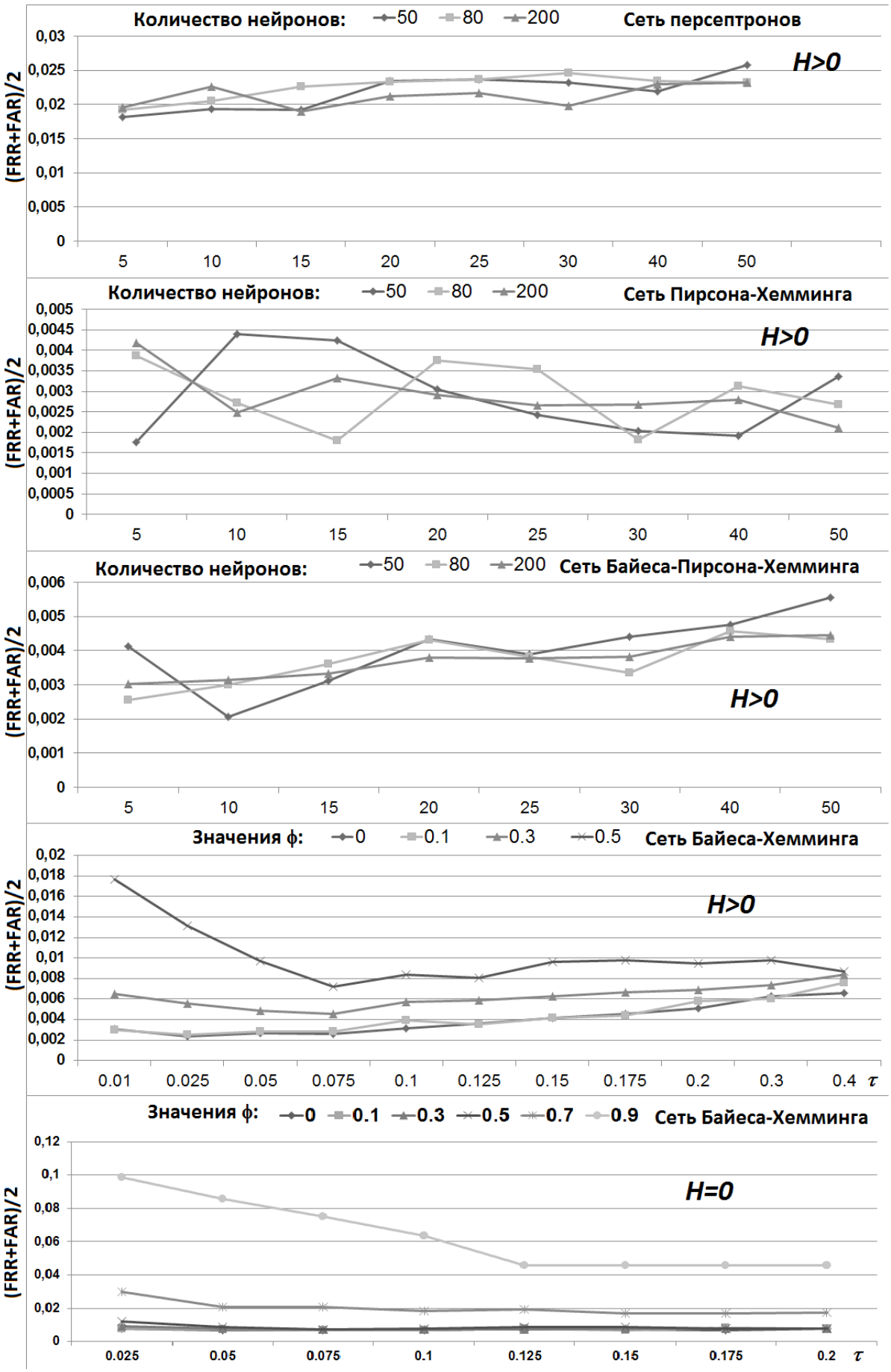

Рис. 4. *Вероятности ошибок верификации испытуемых по лицу при времени мониторинга стандартного оборудования 30 секунд*

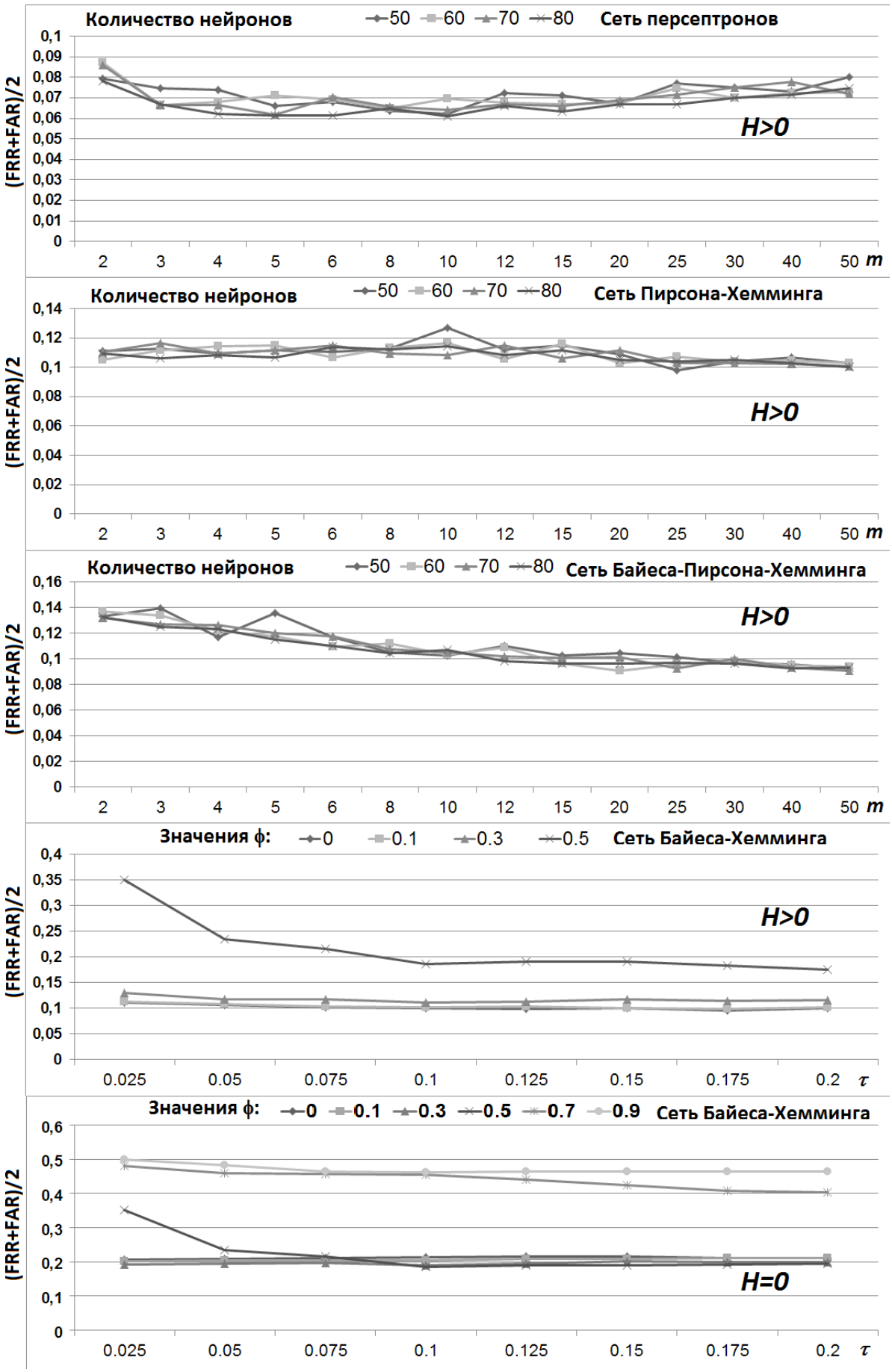

Рис. 5. *Вероятности ошибок верификации испытуемых по клавиатурному почерку при времени мониторинга стандартного оборудования 30 секунд.*

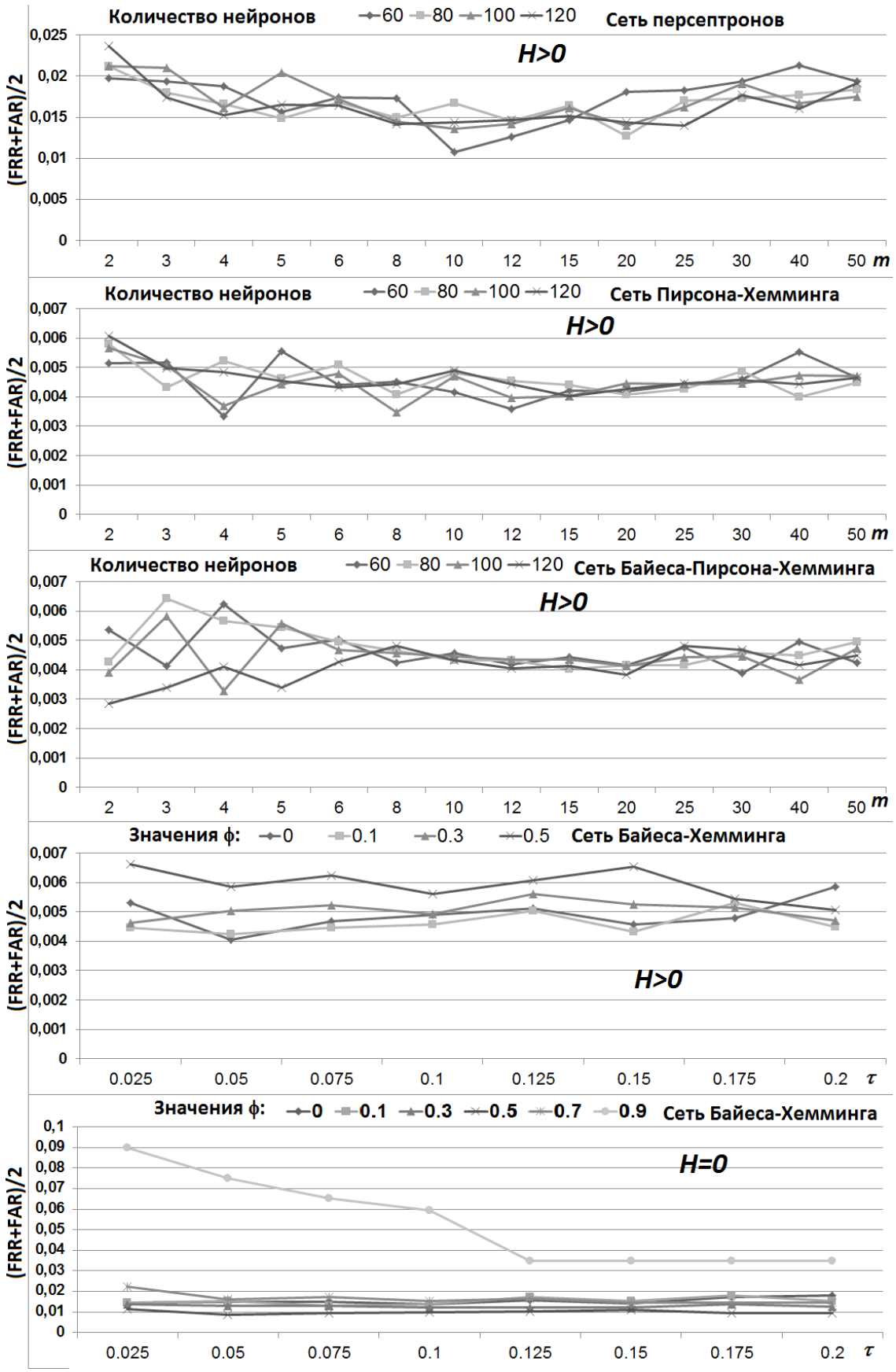

***Рис. 6**. Вероятности ошибок верификации испытуемых по лицу и клавиатурному почерку при времени мониторинга стандартного оборудования 30 секунд.*

Для различных признаков могут быть найдены функционалы, наилучшим образом работающие с ними. Подбирать функционалы целесообразно исходя из взаимной корреляции между признаками и площадей пересечения плотностей вероятности их значений. Экспериментально подтвержден тезис о том, что многомерный функционал Байеса работает тем лучше, чем выше коэффициент равной коррелированности признаков и выше его размерность.

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э. Баумана. E-mail: v.tsirlov@cnpo.ru*

Литература

1. Moving forward with cybersecurity and privacy. (Режим доступа: http://www.pwc.ru/ru/riskassurance/publications/assets/gsiss-report_2017_eng.pdf, дата обращения: 11.12.2016).
2. Васильев В.И., Ложников П.С., Сулавко А.Е., Жумажанова С.С. Оценка идентификационных возможностей биометрических признаков от стандартного периферийного оборудования // Вопросы защиты информации / ФГУП «ВИМИ». - Москва: 2016, №1, С. 12-20.
3. P. Viola and M. Jones. Rapid object detection using a boosted cascade of simple features. Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on. pp I, 511 , I, 518 vol.1. 2001 .
4. Cho, H. & Hwang, SY. J. High-performance on-road vehicle detection with non-biased cascade classifier by weight-balanced training // EURASIP Journal on Image and Video Processing, (2015) 2015: 16. doi:10.1186/s13640-015-0074-5.
5. Srinivasa, K.G. & Gosukonda, S. Continuous multimodal user authentication: coupling hard and soft biometrics with support vector machines to attenuate noise // CSI Transactions on ICT, June 2014, Volume 2, Issue 2, pp 129–140. doi:10.1007/s40012-014-0054-4.
6. P. V. C. Hough, A method and means for recognizing complex patterns, U. S. Patent No.3.069.654, (1962).
7. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений / А.И. Иванов. – Пенза: Изд-во Пенз. гос. ун-та, 2000.–188 с.
8. Борисов Р.В., Зверев Д.Н., Сулавко А.Е., Писаренко В.Ю. Оценка идентификационных возможностей особенностей работы пользователя с компьютерной мышью // Вестник Сибирской государственной автомобильно-дорожной академии / СибАДИ. - Омск: СибАДИ, 2015, № 5(45), С. 106-113.
9. Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, In EUROCRYPT, p. 523-540, 2004.
10. Ложников П.С., Сулавко А.Е., Еременко А.В., Волков Д.А. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами // Информационно-управляющие системы / ГУАП, Санкт-Петербург, 2016, №5, С. 73-85.
11. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография. / Алматы: ТОО «ИздательствоLEM», 2014 – 144 с.
12. Безяев А.В., Иванов А.И., Фунтикова Ю.В. Оптимизация структуры самокорректирующегося био-кода, хранящего синдромы ошибок в виде фрагментов хеш-функций // Вестник УрФО. Безопасность в информационной сфере. 2014, № 3(13), С. 4–13.
13. Иванов А. И., Сомкин С. А., Андреев Д. Ю., Малыгина Е. А. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы // Вестник УрФО. Безопасность в информационной сфере, № 2(12), 2014, С. 16-23.
14. Scotti, F., Cimato, S., Gamassi, M., Piuri, V., Sassi, R. Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System // 2008 Annual Computer Security Applications Conference, IEEE. – 2008. – P. 130-139.
15. А.И. Иванов, П.С. Ложников, Е.И. Качайкин. Идентификация подлинности рукописных автографов сетями Байеса-Хэмминга и сетями квадратичных форм // Вопросы защиты информации. - 2015. - № 2. - С. 28-34.
16. Ложников П.С., Иванов А.И., Качайкин Е.И., Сулавко А.Е. Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса // Вопросы защиты информации / ФГУП «ВИМИ». - Москва: 2015, №3, С. 48-54.
17. Иванов А. И. Снижение размеров достаточной для обучения выборки за счет симметризации корреляционных связей биометрических данных / А. И. Иванов, П. С. Ложников, Ю. И. Серикова // Кибернетика и системный анализ. - 2016. - Т. 52, № 3. - С. 49-56.670.

AUTHENTICATION OF COMPUTER USERS IN REAL-TIME BY GENERATING BIT SEQUENCES BASED ON KEYBOARD HANDWRITING AND FACE FEATURES[6]

6 This work was financially supported by RFBR (grant № 16-37-50049)

Lozhnikov P.S.[7], Sulavko A.E.[8], Buraya E.V.[9], Pisarenko V.Y.[10]

Abstract. We consider the problem of user's recognition in the process of working on a computer in the space of features of keyboard handwriting and face. Several approaches to the formation of solutions is proposed: network of perceptrons and Pearson–Hamming, Bayes–Pearson–Hamming, Bayes–Hamming networks. It was confirmed that the multi–dimensional Bayes functional works better with higher correlated features and when its dimension is higher. It is shown that for a variety features can be found some functional that best work with them. It was found that an increase in user monitoring time can be substantially reduced erroneous decisions due to more accurate calculation of the characteristic values. A method of generating keys (which can be used for encryption, authentication, digital signature algorithm) with probability of erroneous decisions, depending of user monitoring time when he works on a computer was proposed: 30 seconds – FRR = 0,002, FAR = 0,0036; 60 seconds – FRR = 0,002, FAR = 0,0009; 150 seconds – FRR <0,0005, FAR <0,0005.

***Keywords**: keyboard handwriting, facial features, authentication of computer users, recognition of subjects, biometric feature*

References

1. Moving forward with cybersecurity and privacy. (Режим доступа: http://www.pwc.ru/ru/riskassurance/publications/assets/gsiss-report_2017_eng.pdf, дата обращения: 11.12.2016).
2. Vasil'ev V.I., Lozhnikov P.S., Sulavko A.E., Zhumazhanova S.S. Ocenka identifikacionnyh vozmozhnostej biometricheskih priznakov ot standartnogo periferijnogo oborudovanija // Voprosy zashhity informacii / FGUP «VIMI». - Moskva: 2016, №1, P. 12-20.
3. P. Viola and M. Jones. Rapid object detection using a boosted cascade of simple features. Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on. pp I, 511 , I, 518 vol.1. 2001.
4. Cho, H. & Hwang, SY. J. High-performance on-road vehicle detection with non-biased cascade classifier by weight-balanced training // EURASIP Journal on Image and Video Processing, (2015) 2015: 16. doi:10.1186/s13640-015-0074-5.
5. Srinivasa, K.G. & Gosukonda, S. Continuous multimodal user authentication: coupling hard and soft biometrics with support vector machines to attenuate noise // CSI Transactions on ICT, June 2014, Volume 2, Issue 2, pp 129–140. doi:10.1007/s40012-014-0054-4.
6. P. V. C. Hough, A method and means for recognizing complex patterns, U. S. Patent No.3.069.654, (1962).
7. Ivanov A. I. Biometricheskaja identifikacija lichnosti po dinamike podsoznatel'nyh dvizhenij / A.I. Ivanov.– Penza : Izd-vo Penz. gos. un-ta, 2000.–188 p.
8. Borisov R.V., Zverev D.N., Sulavko A.E., Pisarenko V.Ju. Ocenka identifikacionnyh vozmozhnostej osobennostej raboty pol'zovatelja s komp'juternoj mysh'ju // Vestnik Sibirskoj gosudarstvennoj avtomobil'no-dorozhnoj akademii / SibADI. - Omsk: SibADI, 2015, № 5(45), P. 106-113.
9. Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, In EUROCRYPT, p. 523-540, 2004.
10. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Jeksperimental'naja ocenka nadezhnosti verifikacii podpisi setjami kvadratichnyh form, nechetkimi jekstraktorami i perseptronami // Informacionno-upravljajushhie sistemy / GUAP, Sankt-Peterburg, 2016, №5, P. 73-85.
11. Ahmetov B.S., Ivanov A.I., Funtikov V.A., Bezjaev A.V., Malygina E.A. Tehnologija ispol'zovanija bol'shih nejronnyh setej dlja preobrazovanija nechetkih biometricheskih dannyh v kod kljucha dostupa: Monografija. / Almaty: TOO «Izdatel'stvoLEM», 2014 – 144 p.
12. Bezjaev A.V., Ivanov A.I., Funtikova Ju.V. Optimizacija struktury samokorrektirujushhegosja bio-koda, hranjashhego sindromy oshibok v vide fragmentov hesh-funkcij [Bulletin of the Ural Federal District. Security in the field of information] 2014, no. 3(13), pp. 4–13.
13. Ivanov A. I., Somkin S. A., Andreev D. Ju., Malygina E. A. O mnogoobrazii metrik, pozvoljajushhih nabljudat' real'nye statistiki raspredelenija biometricheskih dannyh «nechetkih jekstraktorov» pri ih zashhite nalozheniem gammy // [Bulletin of the Ural Federal District. Security in the field of information], no. 2(12), 2014, pp. 16-23.
14. Scotti, F., Cimato, S., Gamassi, M., Piuri, V., Sassi, R. Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System // 2008 Annual Computer Security Applications Conference, IEEE. – 2008. – P. 130-139.
15. A.I. Ivanov, P.S. Lozhnikov, E.I. Kachaykin. Identifikatsiya podlinnosti rukopisnyih avtografov setyami Bayesa-Hemminga i setyami kvadratichnyih form // Voprosyi zaschityi informatsii [Issues of protection of information] - 2015. - # 2. - S. 28-34.
16. Lozhnikov P.S., Ivanov A.I., Kachaykin E.I., Sulavko A.E. Biometricheskaya identifikatsiya rukopisnyih obrazov s ispolzovaniem korrelyatsionnogo analoga pravila Bayesa // Voprosyi zaschityi informatsii [Issues of protection of information] / FGUP «VIMI». - Moskva: 2015, #3, S. 48-54.
17. Ivanov A. I. Snizhenie razmerov dostatochnoj dlja obuchenija vyborki za schet simmetrizacii korreljacionnyh svjazej biometricheskih dannyh / A. I. Ivanov, P. S. Lozhnikov, Ju. I. Serikova // Kibernetika i sistemnyj analiz. - 2016. - T. 52, № 3. - S. 49-56.670.

7 Lozhnikov Pavel Sergeevich, Ph.D., assistant professor, Omsk State Technical University, Omsk, Russia. E-mail: lozhnikov@gmail.com
8 Sulavko Alexey Evgenievich, Ph.D., Omsk State Technical University, Omsk, E-mail: sulavich@mail.ru
9 Buraya Ekaterina Viktorovna, Ufa State Aviation Technical University (USATU), Ufa, Россия. E-mail: burka-777@yandex.ru
10 Pisarenko Viktor Yurievich, Omsk State Technical University, Omsk, Россия. E-mail: j-e-d-y@mail.ru