ПРОЕКТ ТРЕТЬЕГО НАЦИОНАЛЬНОГО СТАНДАРТА РОССИИ ПО БЫСТРОМУ АВТОМАТИЧЕСКОМУ ОБУЧЕНИЮ БОЛЬШИХ СЕТЕЙ КОРРЕЛЯЦИОННЫХ НЕЙРОНОВ НА МАЛЫХ ОБУЧАЮЩИХ ВЫБОРКАХ БИОМЕТРИЧЕСКИХ ДАННЫХ

Иванов А.И.[1] Сулавко А.Е.[2]

Цель исследования *– показать, что преобразователь биометрии в код доступа, основанный на больших сетях корреляционных нейронов, позволяет получать на выходе еще более длинный ключ с одновременным обеспечением защиты биометрических данных от компрометации.*

Метод исследования *– использование больших «широких» нейронных сетей с автоматическим обучением для реализации процедуры биометрической аутентификации с обеспечением защиты биометрических персональных данных от компрометации.*

Результаты исследования *– первый национальный стандарт ГОСТ Р 52633.5 по автоматическому обучению сетей нейронов был ориентирован только на физически защищенную доверенную вычислительную среду. Защита параметров обученных нейросетевых преобразователей биометрия-код с помощью криптографических методов привела к необходимости использования коротких ключей и паролей при биометрико-криптографической аутентификации. Предлагается строить специальные корреляционные нейроны в мета-пространстве признаков Байеса-Минковского более высокой размерности. Проведен эксперимент по верификации образов клавиатурного почерка при помощи преобразователя биометрия-код на основе набора данных проекта AIConstructor. В мета-пространстве признаков вероятность ошибки верификации оказалась меньше (EER=0,0823), чем в исходном пространстве признаков (EER=0,0864), при этом в защищенном режиме исполнения преобразователя биометрия-код длину ключа удается повысить более чем в 19 раз. Эксперименты показали, что переход в мата-пространство признаков Байеса-Минковского не ведет к проявлению проблемы «проклятья размерности», если часть исходных признаков имеет заметную или сильную взаимную корреляцию. Проблема обеспечения конфиденциальности параметров обученных нейросетевых контейнеров, из которых формируется нейросетевой преобразователь биометрия-код, актуальна не только для задач биометрической аутентификации. Видится возможным разработать стандарт для защиты искусственного интеллекта на базе автоматически обучаемых сетей корреляционных нейронов Байеса-Минковского.*

Ключевые слова: *машинное обучение, распознавание образов, анализ корреляционных связей между признаками, мета-пространство признаков Байеса-Минковского, защита конфиденциальной информации в базах знаний от компрометации, защищенное исполнение искусственного интеллекта, высоконадежная аутентификация.*

DOI:10.21681/2311-3456-2021-3-84-93

Введение

На сегодняшний день в мире остро стоит проблема защиты знаний искусственного интеллекта в ответственных приложениях информационной безопасности. США и страны Евросоюза активно внедряют свои технологические решения по криптографии, биометрии, искусственному интеллекту в качестве международных стандартов. Для этой цели с 1989 по 2016 годы были созданы международные технические комитеты (ТК) по стандартизации ISO/IEC JTC1: sc27 «Защита информации и приватности», sc37 «Биометрия», sc42 «Искусственный интеллект».

Инициативы России по созданию международных стандартов на нейросетевую биометрию и искусственный интеллект, защищенные при помощи российских криптографических методов ни Польша, ни Германия, ни Англия не могут одобрить и поддержать. Чтобы сохранить суверенитет на биометрико-криптографическую защиту Россия вынуждена создавать национальные стандарты по защите биометрических данных граждан и баз знаний искусственного интеллекта, опираясь на собственные научные школы.

1 Иванов Александр Иванович, доктор технических наук, профессор кафедры «Технические средства информационной безопасности» Пензенского государственного университета, научный консультант АО «Пензенский научно-исследовательский электротехнический институт», Пенза, Россия. E-mail: bio.ivan.penza@mail.ru

2 Сулавко Алексей Евгеньевич, кандидат технических наук, доцент кафедры комплексной защиты информации, ФГБОУ ВО Омский государственный технический университет (ОмГТУ), г. Омск, Россия. E-mail: sulavich@mail.ru

Ранее США были безусловными лидерами по биометрическим технологиям. Эпохальным событием для технологий биометрии стало появление в 1998 году национальной спецификации США БиоАПИ, которая позднее была переведена в ранг международного стандарта ГОСТ Р ИСО/МЭК 19784-1-2007. Однако при первом публичном обсуждении БиоАПИ в 1996 году всплыла проблема защиты биометрических шаблонов. Разработчикам БиоАПИ удалось быстро успокоить биометрико-криптографическую общественность перспективами создания в ближайшие два-три года технологии гомоморфного шифрования. Тем не менее, первый стандарт ISO/IEC 18033-6:2019 по гомоморфному шифрованию появился только через 23 года. Данный стандарт не касается шифрования параметров нейросетевых решающих правил. Для защиты обученного искусственного интеллекта и нейронных сетей с помощью гомоморфного шифрования следует разработать отдельные стандарты или рекомендации, которых на данный момент не предложено. Возможная причина кроется в том, что реализация полного гомоморфизма на практике наталкивается на ряд проблем. Основная проблема заключается в низкой производительности [1, 2]. Кроме того, распознавание образов в защищенном с помощью гомоморфного шифрования режиме имеет тенденцию к повышению количества ошибочных решений [3]. Ситуация может объясняться тем, что гомоморфные шифротексты длинных решающих правил перестают расшифровываться после выполнения достаточно большого числа операций сложения и умножения [4]. Однозначное дешифрование оказалось выполнимо только при ограниченном числе операций сложения и умножения, т.е. только для относительно простых решающих правил, усложнение которых приводит к проблемам дешифрования. Может быть, эти проблемы будут решены в будущем (когда – неизвестно). Но уже сегодня требуется обеспечивать надежную защиту биометрических данных и баз знаний искусственного интеллекта, что можно реализовать с помощью новых специальных моделей нейронов и совместимых с ними схем защиты на базе классического шифрования.

Цель исследования – показать, что преобразователь биометрии в код доступа, основанный на больших сетях корреляционных нейронов, позволяет получать на выходе достаточно длинный для всех практических задач криптографический ключ при низком проценте ошибок 1-го и 2-го рода с обеспечением защиты биометрических данных от компрометации. В связи с этим предлагается создать проект третьего национального стандарта на базе автоматически обучаемых сетей корреляционных нейронов.

1. Дополнительная защита данных, построенная на использовании больших сетей искусственных нейронов с линейным накоплением

Одним из способов защиты биометрических данных пользователей является отказ от использования легко интерпретируемых биометрических шаблонов БиоАПИ через применение больших сетей искусственных нейронов. Можно рассматривать такой переход как определенного рода маскирование чувствительной информации. Фактически мы заменяем легко читаемые биометрические шаблоны на гораздо более сложно интерпретируемые таблицы связей и весовых коэффициентов искусственных нейронов.

Первый в мировой практике стандарт ГОСТ Р 52633.5-2011 по быстрому автоматическому обучению больших нейронных сетей (нейросетевых преобразователей биометрия–код или НПБК) на малых выборках биометрических данных пользователя (класс образов «Свой») создан в России. Почему нужен именно автомат, обучающий нейросеть? Потому, что нейросеть должна обучаться в защищенной среде самим пользователем (не специалистом по анализу данных или информационной безопасности). К конфиденциальным биометрическим образам и криптографическим ключам нельзя допускать сторонних людей. Примеры образа «Свой» и криптографический ключ, на которых выполнялось обучение, должны быть уничтожены сразу после обучения в соответствии с ГОСТ Р 52633.0-2006.

Если дополнить два отечественных стандарта (ГОСТ Р 52633.5 и ГОСТ Р 52633.0) национальными криптографическими стандартами России, то мы получаем надежное техническое решение для физически защищенной вычислительной среды. Такое решение уже разработано и положено в основу технической спецификации «Системы обработки информации. Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов», которая принята голосованием 19.11.2020 на 25 заседании ТК 26 «Криптографическая защита информации».

Если сторонние лица не могут видеть операции над биометрическими данными, выполняемые нейронной сетью и порождающие ключ длинной в 256 бит, то этого вполне достаточно для обеспечения безопасной биометрико-криптографической аутентификации пользователей и формирования электронной подписи (ЭП) с биометрической активацией (в соответствии с ГОСТ Р 34.10-2012 длина ключа ЭП должна составлять 256 бит). Однако, как только данные промежуточных вычислений оказываются вне доверенной вычислительной среды, положение меняется. Если сторонний наблюдатель знает таблицы связей нейронов, то он может организовать атаку Г.Б. Маршалко [5]. Атака становится эффективной, если 256 нейронов удается сгруппировать в 1, 2, …. , N групп нейронов с общими входными связями внутри каждой из группы. Так если анализ связей приводит к получению всего N= 5 групп, то вычислительная сложность подбора ключа снижается от перебора 2^{256} состояний до 2^5 состояний. Как результат искусственные нейроны с линейным накоплением данных, обученные по алгоритму ГОСТ Р 52633.5 не должны иметь общих связей. Если нейросеть будет анализировать 512 биометрических параметров, а каждый нейрон будет иметь 16 входов (как правило, этого достаточно), то мы получим всего 512/16=32 искусственных нейронов, каждый из которых продуцирует на выходе один бит информации. То есть шифрование таблиц связей нейронов и их весовых коэффициентов по соответствующей

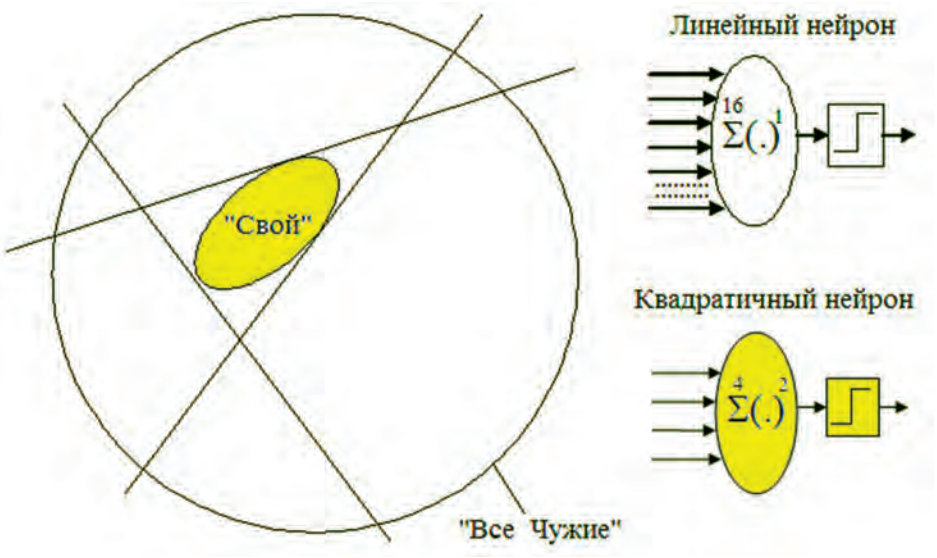

Рис.1. Один квадратичный нейрон с эллиптической границей квантователя данных эквивалентен по своей эффективности примерно трем-четырем линейным нейронам

технической спецификации дает ключ аутентификации длинной 32 бита. Несложно посчитать, длину ключа для реальных примеров реализации методов биометрической аутентификации, когда используется 782 или 521 признаков [6], а также 416 признаков [7] (длина ключа для этих случаев составляет от 26 до 48 бит).

2. Сложности применения методов глубокого обучения для построения защищенного режима исполнения искусственного интеллекта и преобразователей биометрия-код

Многие исследователи стараются использовать преимущества методов глубокого обучения многослойных нейронных сетей в задачах получения ключей из биометрических данных. Отметим, что создать ПБК на основе многослойной нейронной сети с использованием итерационных алгоритмов обучения на сегодняшний день затруднительно [6], так как практически все итерационные алгоритмы имеют существенную склонность к переобучению. Как следствие, приходится постоянно следить за процессом обучения и периодически проводить проверку качества решений на валидационной выборке. Чем ниже информативность биометрического образа (т.е. уникальность и стабильность признаков), тем больший объем обучающей выборки нужен и тем выше склонность к переобучению. Например, для обучения сверточных нейронных сетей в задаче биометрической идентификации личности по лицу [8] достаточно пяти примеров изображения лица от каждого идентифицируемого субъекта. А в задаче верификации подписей обучающая выборка возрастает до 15-30 примеров на подписанта [9], при этом точность распознавания разных подписантов уже сильно варьируется, а процесс обучения теряет робастность. При верификации диктора увеличение числа обучающих примеров может вызвать повышение EER [10], что как раз говорит о неустойчивости обучения. Тем не менее, известны работы [11, 12], в которых сообщается об успешном опыте создания нейросетевых ПБК на основе многослойных сверточных нейронных сетей (пока что это касается приложений лицевой биометрии). Недостаток этих работ (при всех положительных аспектах) заключается в том, что созданный нейросетевой ПБК является жестко зависимым от задачи. Автоматический синтез многослойной нейронной сети с оптимальной конфигурацией под заданную обучающую выборку – крайне сложная научная задача, которая не имеет эффективных решений на данный момент. Так что говорить о создании стандарта на базе методов глубокого обучения не приходится, в силу того, что повторить опыт авторов [11, 12] в другой задаче классификации затруднительно.

3. Второй национальный стандарт России по автоматическому обучению сетей квадратичных нейронов

Следует отметить, что многообразие искусственных нейронов велико. Например, вместо искусственных нейронов с накоплением данных (суммированием) в линейном пространстве могут быть использованы нейроны с накоплением данных в квадратичном пространстве [13]. Ситуация перехода от одних нейронов к другим отображена на рисунке 1.

Сети квадратичных нейронов обучаются в полностью автоматическом режиме. Они имеют общие черты с сетями радиально-базисных функций, однако в отличие от последних не компрометируют биометрический эталон. Квадратичные нейроны имеют иную архитектуру, что позволяет скрывать статистические моменты признаков, вычисляемых при обучении (математические ожидания и среднеквадратичные отклонения).

Квадратичный нейрон с четырьмя входами дает эффект, сравнимый с линейным нейроном, имеющим 16

входов. Таким образом, при обработке 512 признаков сеть квадратичных нейронов будет давать на выходе 512/4=128 бит ключа (каждый нейрон по одному биту). Это существенный рост длины криптографического ключа, но этого во многих случаях недостаточно. В реальных задачах количество входов нейрона зависит от информативности признаков и их коррелированности [14]. Для построения преобразователя биометрического образа в 256 битный ключ требуется не менее 1024 достаточно информативных признаков. Но во многих типах биометрических образов такого количества признаков просто нет [15].

4. Углубление нейро-статистического анализа за счет учета корреляционных связей параметров биометрического образа «Свой»

Все потенциальные меры близости, которые могут лежать в основе квадратичных нейронов и сетей радиально-базисных функций обобщаются с помощью меры Минковского (1) [16]:

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

где a_j – значение j-го признака из вектора $\bar{a}$, представляющего собой распознаваемый образ (биометрический или иной); n – количество признаков, m_j и σ_j – математическое ожидание и среднеквадратичное отклонение значений j-го признака для того класса образов, с которым сравнивается образ $\bar{a}$, p – степенной неотрицательный коэффициент, определяющий уровень «искривления» пространства. Искривление пространства признаков возникает из-за наличия корреляционных связей между ними [16]. Изменяя параметр p можно добиться снижения количества ошибок классификации, если признаки имеют невысокий и примерно равный уровень коррелированности [16]. В реальных задачах корреляция между признаками различна, поэтому следует создавать сеть или комитет [17] нейронов (в данном случае квадратичных), каждый из которых обрабатывает отдельный набор признаков, имеющих определенный в некотором интервале уровень корреляционной зависимости.

Когда уровень корреляционной зависимости между признаками высокий, следует использовать для обработки многомерные (разностные [18], гиперболические [19]) Байесовские функционалы [14]. Эти меры близости обобщаются аналогичным образом с помощью метрики Байеса-Минковского (2), впервые предложенной в работе [16]:

$$y_t = \sqrt[s]{\sum_{j=1}^{n}\left|\left|\frac{(m_t - a_t)}{\sigma_t}\right|^p - \left|\frac{(m_j - a_j)}{\sigma_j}\right|^p\right|}, j \neq t, \qquad (2)$$

где s – «обратный» степенной неотрицательный коэффициент, который может быть равным p, но может и иметь другое значение (обычно s=1). Эта мера принимает тем меньшие значения, чем выше коэффициент корреляции между t-м и j-м. Исследования показали [16], что чем ниже взаимная коррелированность признаков, тем меньше ошибок допускает метрика (2), при этом меняя степенной коэффициент p, можно дополнительно снизить процент ошибок. В приведенном виде мера близости Байеса-Минковского компрометирует эталон пользователя (так как параметры m_j и σ_j нужно где-то хранить). Однако можно перейти к иному варианту этой меры (3), вообще не компрометирующей пользовательские данные [20]:

$$y_t = \sqrt[s]{\sum_{j=1}^{n}\left|\left|\frac{a_t}{\delta_t}\right|^p - \left|\frac{a_j}{\delta_j}\right|^p\right|}, j \neq t, \qquad (3),$$

где δ_j – это нормирующий коэффициент, который не компрометирует данные какого-либо класса, так как это интегральная оценка разброса значений признака для всех классов, не принадлежащих классу «Свой» (далее «Чужие»), таким образом обеспечивается дифференциальная конфиденциальность (можно добавить к δ_j шум, чтобы немного сместить его значение).

Можно перед отправкой данных в сеть нейронов Байеса-Минковского производить нормировку пространства признаков и конвертацию вектора признаков в мета-признаки с помощью отображения (4):

$$a'_{t,j} = f(a_t, a_j) = \left|\frac{a_t}{\delta_t}\right|^p - \left|\frac{a_j}{\delta_j}\right|^p, j \neq t, \qquad (4),$$

тогда мы перейдем в мета-пространство признаков Байеса-Минковского непосредственно [16], в котором можно строить любые классификаторы, способные разделять входные данные по уровню коррелированности. Исследования показали, что мета-признаки содержат иную информацию, не включенную в исходные признаки [16]. Полное количество мета-признаков равно $n'=0{,}5n^2 - 0{,}5n$. Таким образом, при количестве признаков n=512 мы имеем n'=130816 мета-признаков. Также можно видеть, что меры (2) и (3) являются линейными «безвесовыми» классификаторами в мета-пространстве признаков Байеса-Минковского. Нейрон на базе меры близости (2) или (3) назовем корреляционным (или автокорреляционным) нейроном, так как он способен анализировать корреляционные связи между признаками вместо значений признаков в задачах классификации образов.

5. Экспериментальная оценка вероятностей ошибок верификации подписантов в пространстве признаков Байеса-Минковского с помощью НПБК, обучаемых по ГОСТ Р 52633.5

Мы предлагаем строить новый (третий) национальный стандарт России по быстрому автоматическому обучению больших нейронных сетей на основе корреляционных нейронов на базе «безвесовой» метрики Байеса-Минковского (3). Однако для этого требуется разработать алгоритм автоматического синтеза и обучения сети корреляционных «безвесовых» нейронов. Каждый такой нейрон в перспективе должен иметь

Таблица 1

Наилучшие результаты эксперимента (КП – клавиатурный почерк)

Число входов нейрона	Число нейронов	Признаки	EER
6	256	Исходные (n=63)	0,0884
10	***256***	***Исходные (n=63)***	***0,0864***
10	***1024***	***Исходные (n=63)***	***0,0885***
12	256	Исходные (n=63)	0,0939
16	256	Исходные (n=63)	0,1006
10	256	Мета-признаки (n'=1953)	0,0984
12	256	Мета-признаки (n'=1953)	0,0908
16	***256***	***Мета-признаки (n'=1953)***	***0,0891***
16	***1024***	***Мета-признаки (n'=1953)***	***0,0823***
32	256	Мета-признаки (n'=1953)	0,0975

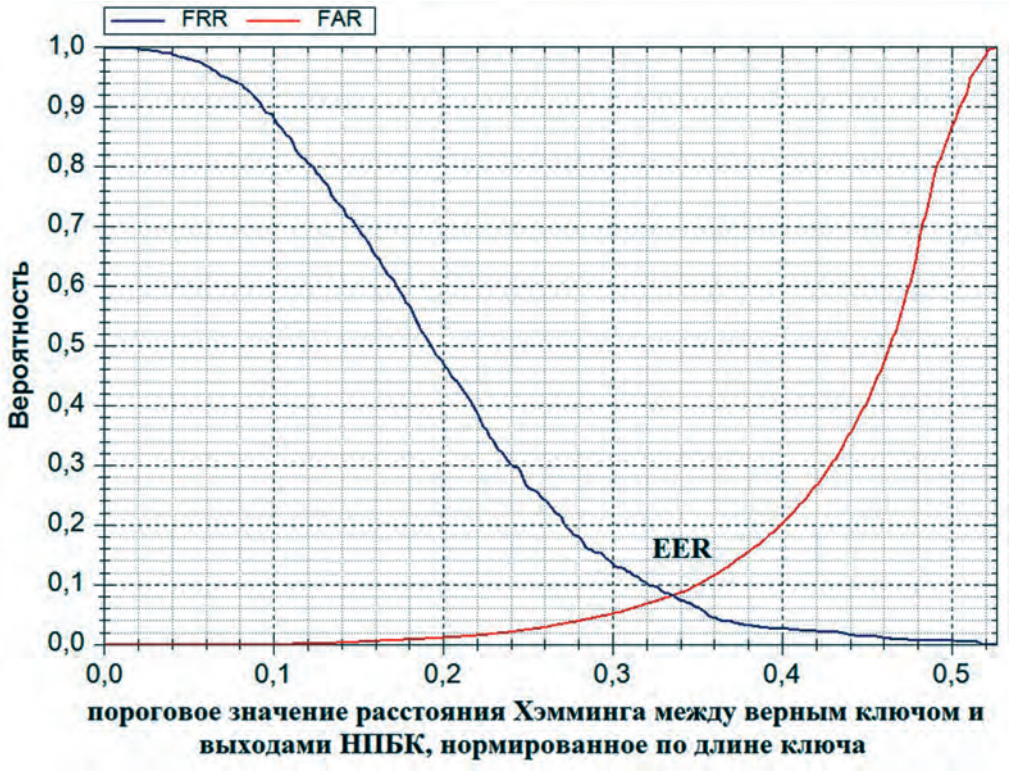

Рис.2. Наилучший результат получен в мета-пространстве признаков Байеса-Минковского при количестве нейронов 1024 и входов нейронов 16

пороги активации. Для защищенного режима исполнения следует использовать пороговую функцию активации с множеством квантователей, так чтобы на выходе нейрона могли возникать более двух бинарных состояний. Это просто необходимо для защиты от ряда атак, которые направлены на извлечение знаний из классического НПБК [21]. Эти пороги должны быть либо стандартные (при условии предъявления требований к балансировке признаков по коэффициентам корреляции) либо настраиваться автоматически, не компрометируя обучающую выборку. Также должны автоматически определяться таблицы связей нейронов с признаками, исходя из корреляционной матрицы признаков.

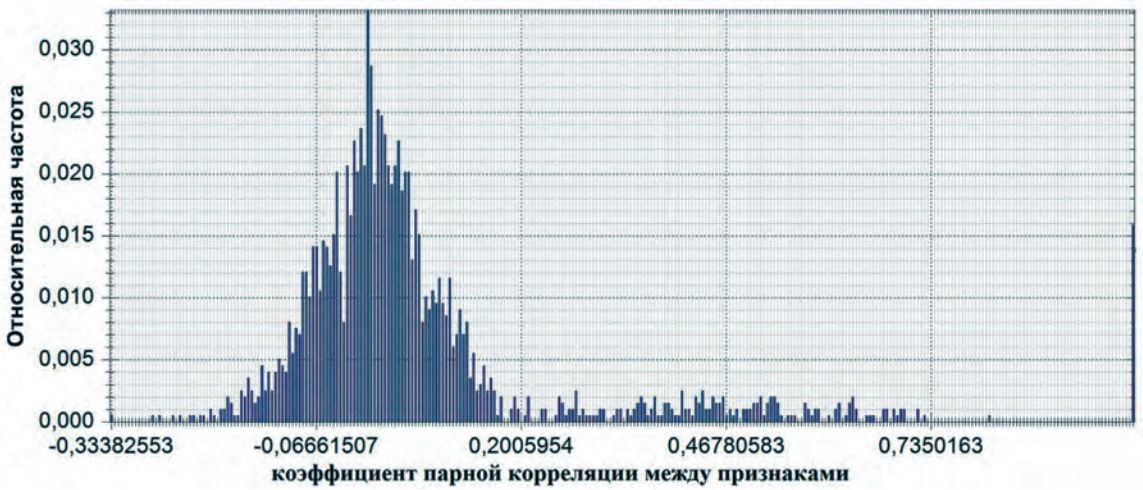

Рис.3. Распределение коэффициентов корреляции между признаками из проприетарного обезличенного набора данных клавиатурного почерка 32 испытуемых, собранного в рамках проекта AIConstructor

Однако для начала нужно протестировать, насколько мета-пространство признаков Байеса-Минковского в целом пригодно для использования в задачах классификации и построения НПБК. В первом приближении это можно сделать, если перейти в мета-пространство с помощью отображения (4) при p=1 и s=1 и построить в нем НПБК без криптографической защиты, обученный по ГОСТ Р 52633.5. Далее стоит обучить аналогичный НПБК, но в пространстве исходных признаков и сравнить результаты. Отличие классических нейронов, на основе которых строится НПБК по ГОСТ Р 52633.5 (помимо использования обычных признаков) заключается в том, что классические нейроны имеют веса входов, в отличии от метрики (3). Тем не менее, возможно, что при использовании мета-признаков для обучения НПБК вместо исходных признаков, защищенность обученных НПБК возрастает. Отпадает необходимость в хранении параметров весов, вычисленных на основе статистических моментов признаков, а вместо них требуется хранить веса, вычисляемые исходя из статистических моментов разниц между признаками (4).

Для этой цели проведен эксперимент с использованием обезличенного набора данных клавиатурного почерка проекта AIConstructor[3], который также использовался в работе [17]. Набор данных содержит образы 32 испытуемых, каждый из которых 50 раз ввел на клавиатуре фразу «система защиты должна постоянно совершенствоваться», учтены только попытки безошибочного ввода. Количество признаков составляет n=63, а мета-признаков – n'=1953. Для каждого испытуемого были созданы НПБК, обучаемые на 20 случайных примерах «Свой» и 31 случайном примере «Чужих» (бралось по одному примеру всех остальных испытуемых, считалось, что все испытуемые по отношению друг к другу «Чужие»). В биометрических системах эти показатели принято называть вероятностями (или процентом) ошибок «ложного отказа» (FRR) и «ложного допуска» (FAR). Сравнение биометрических систем часто выполняется по коэффициенту равной вероятности ошибок (EER=FRR=FAR). Результаты эксперимента можно видеть на рисунке 2 и в таблице 1. Преимущество мета-пространства признаков Байеса-Минковского по отношению к НПБК заключается в том, что можно создать большее число нейронов, тогда длина ключа становится многократно выше 256 бит при использовании однослойного НПБК.

На рисунке 3 можно видеть распределение коэффициентов корреляции между исходными признаками набора данных. Видно, что коэффициентов заметной или высокой корреляции сравнительно немного. Тем не менее, это позволяет получать сравнимую вероятность ошибочных решений в мета-пространстве признаков Байеса-Минковского.

Не смотря на то, что набор данных весьма ограничен в объеме, и эксперимент проведен в «упрощенных» условиях (например, требования к обучающей и тестовой выборкам «Чужих» из ГОСТ Р 52633 выполнены не в полной мере из-за ограниченности объема набора), он позволяет сделать однозначный вывод: мета-пространство признаков Байеса-Минковского является информативным, видимо, даже более информативным, чем исходное.

Выводы

Мы наблюдаем очевидное преимущество темпов развития отечественных стандартов по нейро-криптографической защите биометрических данных. На сегодняшний день нет стандартов (как международных, так и российских), которые бы регламентировали технические аспекты защиты искусственного интеллекта от угрозы реализации всего множества атак, рассмотренных в настоящем отчете. Также пока не удалось разработать и стандартизовать достаточно универсальный для многих приложений метод защиты искусственных нейронных сетей методами гомоморфного шифрования.

Для решения обозначенных проблем требуется разработать иные модели искусственных нейронов и сетей, позволяющих повысить длину ключа в соответствии

3 Наборы данных проекта AIConstructor // AIConstructor: сайт URL: http://aiconstructor.ru/page14247028.html (дата обращения: 12.04.2021)

с текущими требованиями (например, в соответствии с ГОСТ Р 34.10-2012 длина ключа электронной подписи должна составлять 256 бит) или выше (на перспективу), которые могут быть надежно защищены в ближайшем будущем. Это может быть выполнено усилиями технических комитетов 164 и 362. Безопасность может быть дополнительно усилена криптографическими методами, если в этом будет необходимость. Для нейросетевого ПБК, обучаемого по ГОСТ Р 52633.5 уже разработана спецификация по криптографической защите решающих правил. Но не любые знания можно защитить при помощи данной спецификации. Для новой модели нейросетевых ПБК может потребоваться адаптация данной спецификации или разработка новой, а возможно целесообразности в криптографической защите не будет. Эти вопросы будут рассматриваться техническим комитетом №26.

Если перейти от весовых коэффициентов классических нейронов к параметрам корреляционных нейронов, то удается многократно увеличить длину ключа за счет появления множества дополнительных мета-признаков. При этом мета-признаки содержат новую по отношению к исходному пространству признаков информацию. Эксперименты показали, что использование мета-признаков не менее эффективно, чем использование исходных признаков, даже если количество пар заметно и сильно коррелированных признаков (по шкале Чеддока) незначительно.

Перейти в мета-пространство признаков Байеса-Минковского не составляет труда. Эксперименты показывают, что переход в мета-пространство признаков не ведет к проявлению проблемы «проклятья размерности», если признаки коррелированы. Проклятие размерности — это проблема, связанная с экспоненциальным ростом объема обучающей выборки и связанных с этим вычислений из-за линейного роста размерности пространства признаков. Но когда признаки сильно коррелированы, то при использовании аналогичной обучающей выборки (например, 20 примеров) удается достичь более высоких результатов, если перейти в более высокоразмерное пространство мета-признаков Байеса-Минковского. При этом сложность вычислений растет линейно по отношению к увеличению размерности пространства признаков, по крайней мере, при использовании НПБК в качестве классификатора. Количество же признаков при переходе в мета-пространство Байеса-Минковского при этом растет не по экспоненте, а по степенному закону $0{,}5n^2 - 0{,}5n$.

В рассмотренном примере (верификация образов клавиатурного почерка на основе НПБК) даже без криптографической защиты и соответственно без контроля повторения входов нейронов в мета-пространстве признаков Байеса-Минковского при большей длине ключа вероятность ошибки оказалась меньше (EER=0,0823), чем в исходном пространстве признаков (EER=0,0864). При применении криптографической защиты и запрете на наличие одинаковых входов у разных нейронов длина кода для НПБК, обученного в исходном пространстве признаков, составит 6,3 бита (10 входов, 6 полноценных нейронов). Для НПБК, обученного в мета-пространстве признаков, длина ключа составит 122 бита (16 входов, 122 полноценных нейрона). Это очень ощутимое преимущество – более чем в 19 раз поднимается длина ключа при одновременном снижении вероятностей ошибок.

Проблема обеспечения конфиденциальности параметров обученных нейросетевых контейнеров, из которых формируется нейросетевой преобразователь биометрия-код, актуальна не только для задач биометрической аутентификации. Она касается многих ответственных приложений искусственного интеллекта, которые также должны исполняться в защищенном режиме. Видится возможным разработать стандарт для защиты искусственного интеллекта на базе автоматически обучаемых сетей корреляционных нейронов.

Литература

1. Catak, F. O. Privacy-Preserving Fully Homomorphic Encryption and Parallel Computation Based Biometric Data Matching: preprints / F. O. Catak, S. Yildirim Yayilgan, M. Abomhara, 2020. 2020070658. DOI: 10.20944/preprints202007.0658.v1.
2. Multi-biometric template protection based on Homomorphic Encryption / M. Gomez-Barrero [et al.] // Pattern Recognition. 2017. Vol. 67. P. 149–163.
3. A secure face-verification scheme based on homomorphic encryption and deep neural networks / Y. Ma, L. Wu, X. Gu [et al.] // IEEE Access. 2017. Vol. 5. P. 16532–16538.
4. А. О. Жиров, О. В. Жирова, С. Ф. Кренделев. Безопасные облачные вычисления с помощью гомоморфной криптографии // Журнал БИТ (безопасность информационных технологий), том 1, 2013. стр. 6-12.
5. Marshalko, G. B. On the security of a neural network-based biometric authentication scheme / G. B. Marshalko. DOI: https://doi.org/10.4213/mvk120 // Matematicheskie. Voprosy. Kriptografii. 2014. Vol. 5, № 2. P. 87–98.
6. Сулавко, А.Е. Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей // Компьютерная оптика. 2020. Т. 44, № 1. С. 82-91. – DOI: 10.18287/2412-6179-CO-567.
7. Иванов, А. И. Среда моделирования «БиоНейроАвтограф» : программный продукт создан лабораторией биометрических и нейросетевых технологий / А. И. Иванов, О. С. Захаров. 2009 // АО «ПНИЭИ»: офиц. сайт – URL: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip (дата обращения: 07.04.2021).
8. On the Reconstruction of Face Images from Deep Face Templates / Guangcan Mai, Kai Cao, Pong C. Yuen, Anil K. Jain // IEEE Transactions on Pat-tern Analysis and Machine Intelligence. 2019. Vol. 41, no. 5. P. 1188–1202.

9. Hafemann, Luiz G. Writer-independent Feature Learning for Offline Signature Verification using Deep Convolu-tional Neural Networks / Luiz G. Hafemann, Robert Sabourin, Luiz S. Oliveira. DOI: 10.1109/IJCNN.2016.7727521 // International Joint Conference on Neural Networks (IJCNN). 2016. URL: https://ieeexplore.ieee.org/abstract/document/7727521 (date accessed: 07.04.2021)
10. Torfi, Amirsina. Text-independent speaker verification using 3d convolutional neural networks / Amirsina Torfi, Jeremy Dawson, Nasser M. Nasrabadi. DOI: 10.1109/ICME.2018.8486441 // IEEE International Conference on Multimedia and Expo (ICME). 23–27 July 2018. URL: https://ieeexplore.ieee.org/abstract/document/8486441 (date accessed: 07.04.2021)
11. Deep secure encoding for face template protection / R. K. Pandey, Y. Zhou, B. U. Kota, V. Govindaraju. DOI:10.1109/CVPRW.2016.17 // IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Las Vegas, NV, USA 2016. P. 77–83
12. Kumar Jindal, A. Face template protection using deep convolutional neural network / A. Kumar Jindal, S. Chalamala, S. Kumar Jami // IEEE Conference on Computer Vision and Pattern Recognition Workshops. Salt Lake City, UT, USA, 2018. P. 462–470
13. Иванов А. И., Безяев А. В., Малыгина Е. А., Серикова Ю. И. Второй национальный стандарт России по быстрому автоматическому обучению больших искусственных нейронных сетей на малых выборках биометрических данных // Сборник научных статей по материалам I Всероссийской научно-технической конференции «Безопасность информационных технологий», 24 апреля, Пенза 2019, с. 174-177.
14. Ложников, П. С. Биометрическая защита гибридного документооборота: моногр. / П. С. Ложников // Новосибирск : Изд-во СО РАН, 2017. 129 с. ISBN 978-5-7692-1561-2.
15. Сулавко А.Е. Тестирование нейронов для распознавания биометрических образов при различной информативности признаков // Прикладная информатика. 2018. №1. С. 128-143.
16. Sulavko A.E. Bayes-Minkowski measure and building on its basis immune machine learning algorithms for biometric facial identification // Journal of Physics: Conference Series. - Vol. 1546. - IV International Scientific and Technical Conference «Mechanical Science and Technology Update» (MSTU-2020) 17-19 March, 2020, Omsk, Russian Federation. DOI: 10.1088/1742-6596/1546/1/012103
17. Сулавко, А.Е. Абстрактная модель искусственной иммунной сети на основе комитета классификаторов и ее использование для распознавания образов клавиатурного почерка // Компьютерная оптика. 2020. Т. 44, № 5. С. 830-842. DOI: 10.18287/2412-6179-CO-717
18. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // Вопросы кибербезопасности. 2017. №3. С. 24–34. DOI: 10.21681/2311-3456-2017-3-24-34
19. Ivanov, A. I. Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data / A. I. Ivanov, S. E. Vyatchanin, P. S. Lozhnikov. DOI: 10.1109/SIBCON.2017.7998435 // International Siberian Conference on Control and Communications (SIBCON), 29–30 June 2017. Astana, 2017.
20. Сулавко, А. Е. Высоконадежная аутентификация по рукописным паролям на основе гибридных нейронных сетей с обеспечением защиты биометрических эталонов от компрометации. Информационно-управляющие системы, (4), 2020. 61-77. DOI: 10.31799/1684-8853-2020-4-61-77
21. Bogdanov, D. S. Data recovery for a neural network-based biometric authentication scheme / D. S. Bogdanov, V. O. Mironkin // Математические вопросы криптографии. 2019. Vol. 10, № 2. С. 61–74

DRAFT OF THE THIRD NATIONAL STANDARD OF RUSSIA FOR FAST AUTOMATIC LEARNING OF LARGE CORRELATION NEURAL NETWORKS ON SMALL TRAINING SAMPLES OF BIOMETRIC DATA

Ivanov A.I.[4], Sulavko A.E.[5]

The aim of the study *is to show that a biometrics-to-access code converter based on large networks of correlation neurons makes it possible to obtain an even longer key at the output while ensuring the protection of biometric data from compromise.*

The research method *is the use of large «wide» neural networks with automatic learning for the implementation of the biometric authentication procedure, ensuring the protection of biometric personal data from compromise.*

Results of the study - *the first national standard GOST R 52633.5 for the automatic training of neuron networks was focused only on a physically secure, trusted computing environment. The protection of the parameters of the trained neural network converters biometrics-code using cryptographic methods led to the need to use short keys*

4 Alexander Ivanov, Dr.Sc. (of Tech.), Professor, JSC “Penza Research Electrotechnical Institute”, Penza, Russia. E-mail: bio.ivan.penza@mail.ru

5 Alexeiy Sulavko, Ph.D., Assistant Professor, Omsk State Technical University, Omsk, Russia. E-mail: sulavich@mail.ru

and passwords for biometric-cryptographic authentication. It is proposed to build special correlation neurons in the meta-space of Bayes-Minkowski features of a higher dimension. An experiment was carried out to verify the patterns of kkeystroke dynamics using a biometrics-to-code converter based on the data set of the AIConstructor project. In the meta-space of features, the probability of a verification error turned out to be less (EER = 0.0823) than in the original space of features (EER = 0.0864), while in the protected execution mode of the biometrics-to-code converter, the key length can be increased by more than 19 times. Experiments have shown that the transition to the mat space of Bayes-Minkowski features does not lead to the manifestation of the "curse of dimension" problem if some of the original features have a noticeable or strong mutual correlation. The problem of ensuring the confidentiality of the parameters of trained neural network containers, from which the neural network converter biometrics-code is formed, is relevant not only for biometric authentication tasks. It seems possible to develop a standard for protecting artificial intelligence based on automatically trained networks of Bayesian-Minkowski correlation neurons.

Keywords: *machine learning, pattern recognition, analysis of correlations between features, meta-space of Bayes-Minkowski features, protection of confidential information in knowledge bases from compromise, secure execution of artificial intelligence, highly reliable authentication.*

References

1. Catak, F. O. Privacy-Preserving Fully Homomorphic Encryption and Parallel Computation Based Biometric Data Matching : rreprints / F. O. Catak, S. Yildirim Yayilgan, M. Abomhara, 2020. 2020070658. DOI: 10.20944/preprints202007.0658.v1.
2. Multi-biometric template protection based on Homomorphic Encryption / M. Gomez-Barrero [et al.] // Pattern Recognition. 2017. Vol. 67. R. 149–163.
3. A secure face-verification scheme based on homomorphic encryption and deep neural networks / Y. Ma, L. Wu, X. Gu [et al.] // IEEE Access. 2017. Vol. 5. P. 16532–16538.
4. A. O. Zhirov, O. V. Zhirova, S. F. Krendelev. Bezopasny`e oblachny`e vy`chisleniia s pomoshch`iu gomomorfnoi` kriptografii // Zhurnal BIT (bezopasnost` informatcionny`kh tekhnologii`), tom 1, 2013. str. 6-12.
5. Marshalko, G. B. On the security of a neural network-based biometric authentication scheme / G. B. Marshalko. DOI: https://doi.org/10.4213/mvk120 // Matematicheskie. Voprosy. Kriptografii. 2014. Vol. 5, № 2. P. 87–98.
6. Sulavko, A.E. Vy`sokonadezhnaia dvukhfaktornaia biometricheskaia autentifikatciia po rukopisny`m i golosovy`m paroliam na osnove gibkikh nei`ronny`kh setei` // Komp`iuternaia optika. 2020. T. 44, № 1. S. 82-91. – DOI: 10.18287/2412-6179-CO-567.
7. Ivanov, A. I. Sreda modelirovaniia «BioNei`roAvtograf» : programmny`i` produkt sozdan laboratoriei` biometricheskikh i nei`rosetevy`kh tekhnologii` / A. I. Ivanov, O. S. Zaharov. 2009 // AO «PNIE`I»: ofitc. sai`t – URL: http://pnie`i.rf/activity/science/noc/bioneuroautograph.zip (data obrashcheniia: 07.04.2021).
8. On the Reconstruction of Face Images from Deep Face Templates / Guangcan Mai, Kai Cao, Pong C. Yuen, Anil K. Jain // IEEE Transactions on Pat-tern Analysis and Machine Intelligence. 2019. Vol. 41, no. 5. P. 1188–1202.
9. Hafemann, Luiz G. Writer-independent Feature Learning for Offline Signature Verification using Deep Convolu-tional Neural Networks / Luiz G. Hafemann, Robert Sabourin, Luiz S. Oliveira. DOI: 10.1109/IJCNN.2016.7727521 // International Joint Conference on Neural Networks (IJCNN). 2016. URL: https://ieeexplore.ieee.org/abstract/document/7727521 (date accessed: 07.04.2021)
10. Torfi, Amirsina. Text-independent speaker verification using 3d convolutional neural networks / Amirsina Torfi, Jeremy Dawson, Nasser M. Nasrabadi. DOI: 10.1109/ICME.2018.8486441 // IEEE International Conference on Multimedia and Expo (ICME). 23–27 July 2018. URL: https://ieeexplore.ieee.org/abstract/document/8486441 (date accessed: 07.04.2021)
11. Deep secure encoding for face template protection / R. K. Pandey, Y. Zhou, B. U. Kota, V. Govindaraju. DOI:10.1109/CVPRW.2016.17 // IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Las Vegas, NV, USA 2016. R. 77–83
12. Kumar Jindal, A. Face template protection using deep convolutional neural network / A. Kumar Jindal, S. Chalamala, S. Kumar Jami // IEEE Conference on Computer Vision and Pattern Recognition Workshops. Salt Lake City, UT, USA, 2018. R. 462–470
13. Ivanov A. I., Beziaev A. V., Maly`gina E. A., Serikova Iu. I. Vtoroi` natcional`ny`i` standart Rossii po by`stromu avtomaticheskomu obucheniiu bol`shikh iskusstvenny`kh nei`ronny`kh setei` na maly`kh vy`borkakh biometricheskikh danny`kh // Sbornik nauchny`kh statei` po materialam I Vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasnost` informatcionny`kh tekhnologii`», 24 aprelia, Penza 2019, s. 174-177.
14. Lozhnikov, P. S. Biometricheskaia zashchita gibridnogo dokumentooborota: monogr. / P. S. Lozhnikov // Novosibirsk : Izd-vo SO RAN, 2017. 129 s. ISBN 978-5-7692-1561-2.
15. Sulavko A.E. Testirovanie nei`ronov dlia raspoznavaniia biometricheskikh obrazov pri razlichnoi` informativnosti priznakov // Pricladnaia informatika. 2018. №1. S. 128-143.
16. Sulavko A.E. Bayes-Minkowski measure and building on its basis immune machine learning algorithms for biometric facial identification // Journal of Physics: Conference Series. - Vol. 1546. - IV International Scientific and Technical Conference "Mechanical Science and Technology Update" (MSTU-2020) 17-19 March, 2020, Omsk, Russian Federation. DOI: 10.1088/1742-6596/1546/1/012103
17. Sulavko, A.E. Abstraktnaia model` iskusstvennoi` immunnoi` seti na osnove komiteta classifikatorov i ee ispol`zovanie dlia raspoznavaniia obrazov claviaturnogo pocherka // Komp`iuternaia optika. 2020. T. 44, № 5. S. 830-842. DOI: 10.18287/2412-6179-CO-717
18. Lozhnikov P.S., Sulavko A.E., Buraia E.V., Pisarenko V.Iu. Autentifikatciia pol`zovatelei` komp`iutera na osnove claviaturnogo pocherka i osobennostei` litca // Voprosy` kiberbezopasnosti. 2017. №3. S. 24–34. DOI: 10.21681/2311-3456-2017-3-24-34

19. Ivanov, A. I. Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data / A. I. Ivanov, S. E. Vyatchanin, P. S. Lozhnikov. DOI: 10.1109/SIBCON.2017.7998435 // International Siberian Conference on Control and Communications (SIBCON), 29–30 June 2017. Astana, 2017.
20. Sulavko, A. E. Vy`sokonadezhnaia autentifikatciia po rukopisny`m paroliam na osnove gibridny`kh nei`ronny`kh setei` s obespecheniem zashchity` biometricheskikh e`talonov ot komprometatcii. Informatcionno-upravliaiushchie sistemy`, (4), 2020. 61-77. DOI: 10.31799/1684-8853-2020-4-61-77
21. Bogdanov, D. S. Data recovery for a neural network-based biometric authentication scheme / D. S. Bogdanov, V. O. Mironkin // Matematicheskie voprosy` kriptografii. 2019. Vol. 10, № 2. S. 61–74