УДК 51-37
doi: 10.21685/2072-3059-2024-4-5

Об аппаратно-программной защите приложений доверенного искусственного интеллекта в базисах RNS с интервально-позиционными характеристиками решающих правил

В. С. Князьков[1], А. И. Иванов[2], К. С. Исупов[3], М. М. Бутаев[4]

[1]Пензенский государственный университет, Пенза, Россия
[2]Пензенский научно-исследовательский электротехнический институт, Пенза, Россия
[3]Вятский государственный университет, Киров, Россия
[4]Научно-производственное предприятие «Рубин», Пенза, Россия

[1]kniazkov@list.ru, [2]ivan@pniei.penza.ru, [3]isupov.k.s.work@gmail.com, [4]nts@npp-rubin.ru

Аннотация. *Актуальность и цели.* Целью работы является описание потенциальных преимуществ аппаратно-программной защиты нейросетевых приложений искусственного интеллекта. *Материалы и методы*. В силу универсальности нейросетевых приложений акцентируется внимание на преимуществах представления любых решающих правил искусственного интеллекта через их декомпозицию в форме той или иной архитектуры нейронных сетей. В качестве примера рассматривается задача безопасной биометрической аутентификации личности человека с использованием быстрого алгоритма обучения, рекомендуемого отечественным стандартом ГОСТ Р 52633.5–2011. Отмечается простота программной реализации искусственных нейронов в недоверенной вычислительной среде, так как при реализации многих из них достаточно использования только двух операций: операции сложения «+» и операций умножения «×». Обсуждается перспектива поддержки гомоморфизма по отношению к дополнительным четырем операциями: сравнение чисел, определение знака, переполнение суммирования, переполнение умножения. *Результаты и выводы.* Классические криптографических алгоритмы гомоморфного шифрования содержания решающих правил не могут быть реализованы на основе малопотребляющих USB-карт с программируемыми логическими матрицами. Эта проблема снимается, если для поддержки гомоморфности нейросетевых решающих правил используются компактные некриптографические преобразования, построенные на программировании во множестве систем остаточных классов.

Ключевые слова: гомоморфное шифрование, нейросетевые приложения, программирование в системах остаточных классов, расширение числа гомоморфных математических операций

Для цитирования: Князьков В. С., Иванов А. И., Исупов К. С., Бутаев М. М. Об аппаратно-программной защите приложений доверенного искусственного интеллекта в базисах RNS с интервально-позиционными характеристиками решающих правил // Известия высших учебных заведений. Поволжский регион. Технические науки. 2024. № 4. С. 50–69. doi: 10.21685/2072-3059-2024-4-5

On the hardware and software protection of trusted artificial intelligence applications in RNS bases with interval positional characteristics of decision rules

V.S. Knyazkov[1], A.I. Ivanov[2], K.S. Isupov[3], M.M. Butayev[4]

[1]Penza State University, Penza, Russia

[2]Penza Scientific Research Electrotechnical Institute, Penza, Russia
[3]Vyatka State University, Kirov, Russia
[4]Research and Production Enterprise “Rubin”, Penza, Russia
[1]kniazkov@list.ru, [2]ivan@pniei.penza.ru, [3]isupov.k.s.work@gmail.com, [4]nts@npp-rubin.ru

Abstract. *Background.* The purpose of the study is to describe the potential advantages of hardware and software protection of neural network applications of artificial intelligence. *Materials and methods*. Due to the universality of neural network applications, attention is focused on the advantages of representing any decision rules of artificial intelligence through their decomposition in the form of one or another neural network architecture. As an example, the problem of secure biometric authentication of a person's identity is considered using a fast learning algorithm recommended by the State Standard R 52633.5–2011. The simplicity of software implementation of artificial neurons in an untrusted computing environment is noted, since when implementing many of them it is sufficient to use only two operations: the addition operation «+» and the multiplication operations «×». The prospect of supporting homomorphism with respect to four additional operations is discussed: comparison of numbers, determination of sign, summation overflow, multiplication overflow. *Results and conclusions.* Classical cryptographic algorithms for homomorphic encryption of the content of decision rules cannot be implemented on the basis of low-power USB cards with programmable logic matrices. This problem is removed if compact non-cryptographic transformations based on programming in a set of residual class systems are used to support the homomorphism of neural network decision rules.

Keywords: homomorphic encryption, neural network applications, programming in residual class systems, expanding the number of homomorphic mathematical operations

For citation: Knyazkov V.S., Ivanov A.I., Isupov K.S., Butayev M.M. On the hardware and software protection of trusted artificial intelligence applications in RNS bases with interval positional characteristics of decision rules. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki = University proceedings. Volga region. Engineering sciences.* 2024;(4):50–69. (In Russ.). doi: 10.21685/2072-3059-2024-4-5

Введение

В соответствии с Указом В. В. Путина от 10.10.2019[1] к 2030 г. Россия должна занимать одно из ведущих мест в мире как производитель и потребитель промышленных приложений искусственного интеллекта (ИИ). В связи с этим в 2019 г. был создан в рамках Госстандарта национальный технический комитет № 164 «Искусственный интеллект» (ТК 164), являющийся аналогом международного комитета ISO/IEC JTC1 sc42. За прошедшее время ТК 164 гармонизовал, разработал и ввел в действие на территории РФ порядка 200 национальных стандартов, регламентирующих те или иные аспекты приложений искусственного интеллекта.

Следует также отметить, что в промышленности должны использоваться обязательно «доверенные» приложения искусственного интеллекта. Как минимум, они должны принимать решения с уровнем доверия, объявленным производителем. Вторым важным моментом является гарантия того, что во время промышленного применения никто не сможет исказить (подменить) верное решение доверенного ИИ.

Третьим важнейшим условием применения приложений ИИ является сохранение в тайне их настроек и элементов архитектуры по требованиям

[1] О развитии искусственного интеллекта в Российской Федерации : указ Президента РФ № 490 от 10.10.2019.

действующего законодательства. Например, нейросетевые приложения биометрической аутентификации личности по требованиям ФЗ «О персональных данных»[1] должны быть надежно защищены. Нейросеть, преобразующую биометрию пользователя в код его длинного пароля или личного криптографического ключа, нельзя открыто хранить в недоверенной вычислительной среде обычного компьютера или сотового телефона. Необходимо защищать обученную нейросеть криптографическими механизмами, выполненными по отечественной технической спецификации[2].

Четвертым (рыночным) условием успешного коммерческого применения приложений доверенного ИИ является аппаратно-программная поддержка авторских прав производителя. Нельзя допускать ситуации, когда промышленный потребитель имеет возможность неограниченно копировать приложения ИИ, получая при этом прибыль и не возвращая часть ее производителю.

Практика аппаратной защиты приложений ИИ сегодня существует в двух вариантах. В частности, отечественная компания NtechLab специализируется на распознавании лиц и на видеоаналитике. Свои решения она запаковывает в собственные аппаратные фрагменты, являющиеся аналогами обычных графических ускорителей. Фактически эта компания использует программируемую логическую матрицу (ПЛМ) достаточно большого объема для размещения в ней нейронной сети глубокого обучения [1, 2] с некоторыми особенностями их собственной архитектуры. Аппаратная поддержка нейросетевых решений компании NtechLab одновременно решает две задачи. С одной стороны, она ускоряет вычисления за счет применения аппаратных специализированных вычислителей, а с другой – аппаратные решения защищают интеллектуальную собственность производителя.

Еще одной технологией защиты авторских прав является размещение громоздких приложений нейросетевого ИИ на серверах поставщика услуг. По такому пути пошли компании, владеющие голосовыми секретарями (помощниками): «Алиса» (Яндекс), «Маруся» (Google), «Салют» (СберБанк), «Секретарь» (МТС). В основу этой технологии положены преобразования естественной речи человека в текст. По сути дела, приложение получает через Интернет оцифрованную речь конкретного пользователя и переводит ее в текст поискового запроса.

На рис. 1 приведена концептуальная организация систем ИИ (СИИ), где показаны разнообразные атаки на систему из вне. Более подробно этот вопрос рассмотрен в [3].

Техническая проблема состоит в том, что приложения этого типа огромны, их уже нельзя разместить в рядовом пользовательском компьютере даже с графическим ускорителем. В итоге применяются «облачные» сервисы, владельцы которых не афишируют мощность и энергопотребление «облака» для реализации технологии голосового ассистента. При этом носители «облачных» сервисов должны располагаться на физически защищенной территории. Не каждая компания может себе позволить подобные технологические решения. Перспективным подходом для защиты ИИ от различных типов атак

[1] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

[2] Техническая спецификация ТС 26.2.002–2020 «Системы обработки информации. Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов» URL: https://tc26.ru

является применение доверенной вычислительной среды на базе криптографических технологий гомоморфного шифрования данных (рис. 2).

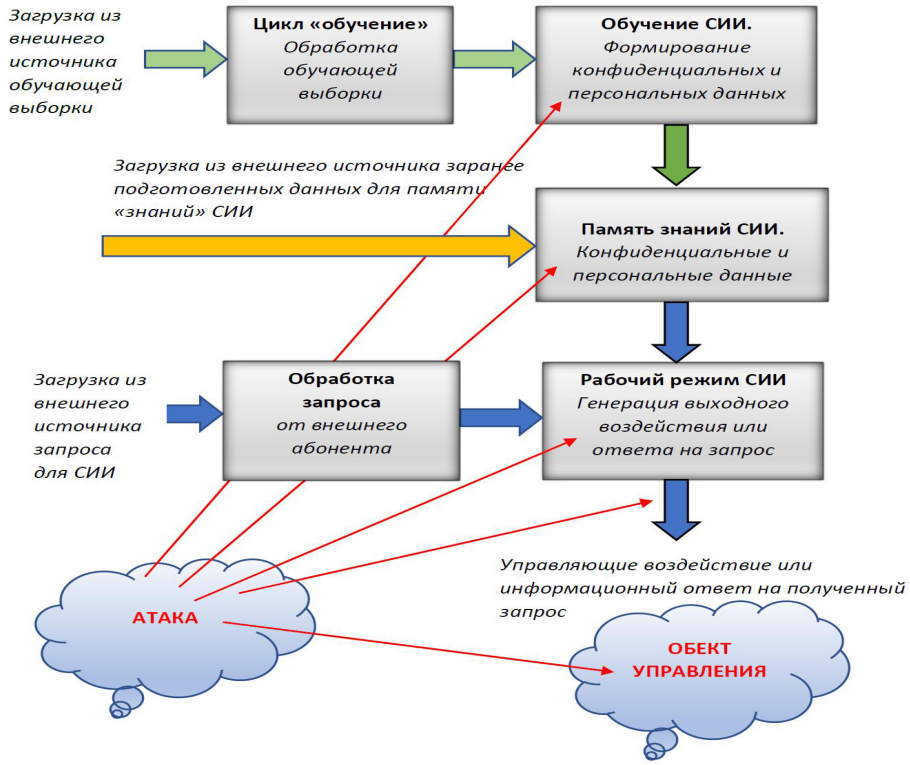

Рис. 1. Виды атак на системы ИИ

При таком подходе требуется выполнять вычисления высокой сложности, что приводит, во-первых, к низкой скорости вычислений[1]; во-вторых, к фатальному накоплению ошибок при расшифровке «длинных рекуррентных» вычислений [4–6]. Кроме этого, возникает необходимость модификации или разработки новых алгоритмов для выполнения вычислений под конкретную криптографическую систему, а в ряде случаев требуется применение специализированного оборудования.

Вторая ключевая проблема – это невозможность реализовать правила обучения и принятия решений, в которых используются не только операции алгебраического сложения и умножения. Например, невозможно реализовать такие функции активации нейронов в нейронных системах ИИ, как функция Хемминга ($F(z)$) или функция Хэвисайда (σ):

$$F(z)=\begin{cases}0, \text{ если } z\le 0,\\ z_i, \text{ если } 0< z\le n,\\ n, \text{ если } z_i > n;\end{cases} \quad (1)$$

[1] ISO/IEC 18033-6:2019. IT Security techniques Encryption algorithms Part 6: Homomorphic encryption. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:18033:-6:ed-l:en (дата обращения: 07.04.2021).

$$\sigma = H(x) = \begin{cases} 1, \text{ если } x > 0, \\ 0, \text{ если } x \le 0. \end{cases} \quad (2)$$

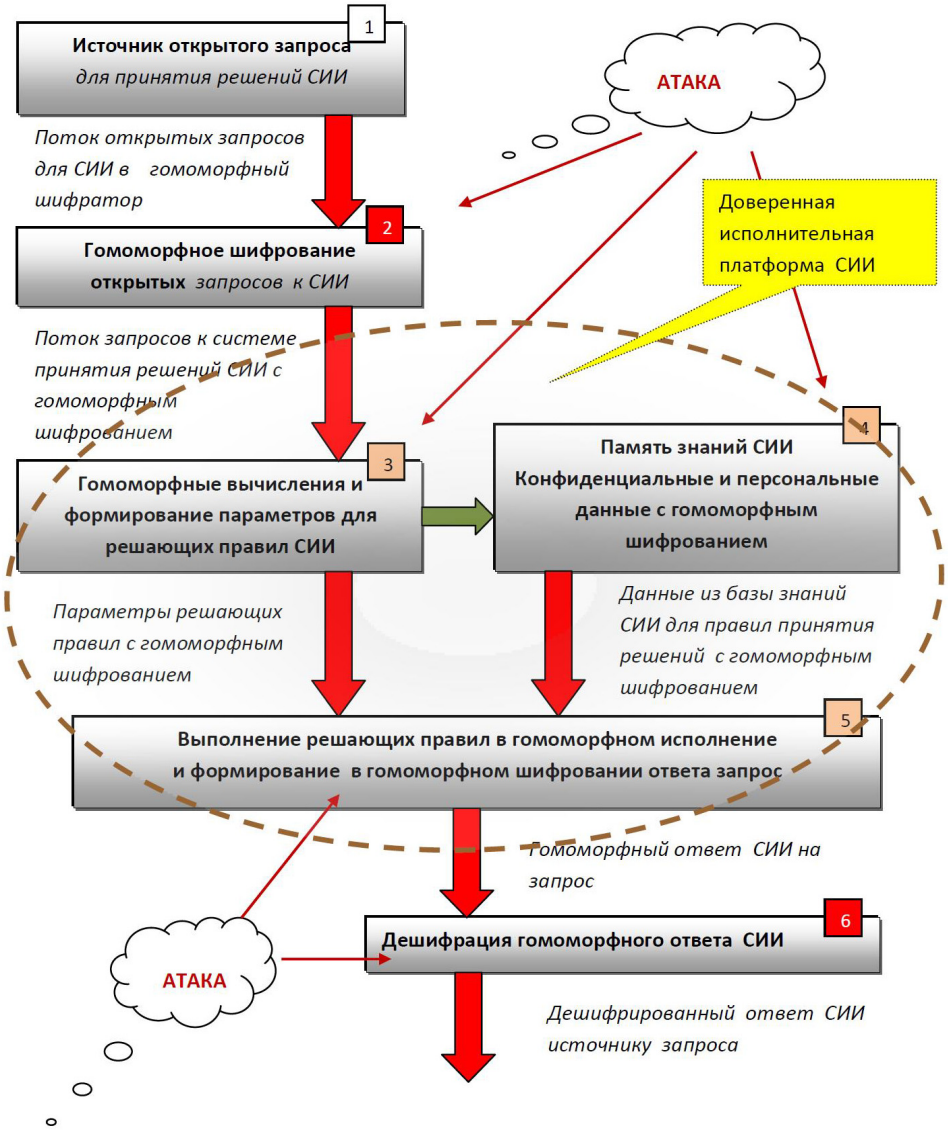

Рис. 2. Концептуальная организация системы ИИ с гомоморфной криптозащитой

В нейросетевых системах ИИ различного назначения также используются радиально-базисных функций активации вида:

- мультиквадратичная функция: $\varphi(r)=\sqrt{1+(\epsilon r)^2}$;
- обратная квадратичная функция:

$$\varphi(r) = \frac{1}{1+(\epsilon r)^2};$$

▪ нейрон квадрата среднего геометрического:

$$\begin{cases} x \leftarrow sort(x), \\ s^2 \leftarrow \sum_{i=0}^{19} \left(\sqrt{\frac{(i+1)\cdot(1-P(x_i)}{21}} \right)^2, \\ z\left(s^2\right) \leftarrow "0" if \ \ s^2 \geq 3,67, \\ z\left(s^2\right) \leftarrow \ "1" if \ \ s^2 < 3,67, \\ P_1 \ \approx P_2 \ \approx P_{EE} \ \approx 0,382. \end{cases}$$

В итоге для реализации системы ИИ требуется выполнять операции деления, сравнения на равенство, больше и меньше, вычисления квадратного корня; вычислять математические выражения.

Цель данной работы – обсудить и показать эффективность применения для защиты систем ИИ некриптографических гомоморфных RNS-систем в остаточных классах.

Материалы и методы

Очевидно, что использовать системы ИИ хотят не только крупные информационные компании. Малые и средние компании хотели бы уже сегодня создавать свои собственные приложения ИИ, в том числе промышленного назначения. Создавать под свои продукты собственные «облака» малые компании не могут (дорого). Возникает потребность создать технологию вычислений, обеспечивающую их безопасность в «облаках». Тогда можно арендовать чужое «облако», например, защитив свои вычисления гомоморфным шифрованием[1].

Если взять некоторый исполняемый на обычном компьютере файл, зашифровать его обычной криптографией, то запустить его на исполнение не получится. Перед тем как его исполнить, его нужно расшифровать. Если это делать в «облаках», то ключ расшифровывания может быть скомпрометирован кем угодно.

Ситуация меняется, если зашифрованный файл можно исполнять без его расшифровывания. Технически это возможно. Гомоморфное шифрование, выполненное по стандарту ISO/IEC 18033-6, не требует шифровать данные и связи решающего правила, но только по отношению к двум математическим операциям: операции сложения «+» и операции умножения «×». При этом не любое решающее правило современного ИИ может быть приведено к этим двум операциям.

Так, международный стандарт по гомоморфному шифрованию ISO/IEC 18033-6 рекомендует выполнять вычисления, опираясь на коды длиной 1024 бита и выше. Это в итоге и приводит к огромному росту энергозатрат при организации вычислений со скрытым смысловым содержанием через

[1] ISO/IEC 18033-6: 2019. IT Security techniques-Encryption algorithms – Part 6: Homomorphic enctyption. 2019. 24 p.

поддержку гомоморфного шифрования, использующего арифметику длинных и сверхдлинных чисел.

Еще одной проблемой гомоморфного шифрования по международному стандарту является то, что приближение функций относительно короткими степенными полиномами дает значительные ошибки $\Delta f(x)$. Эти ошибки приближения быстро накапливаются. В итоге достаточно сложные вычисления, выполняемые при сокрытии их гомоморфным шифрованием, перестают корректно расшифровываться.

В качестве системы счисления для кодирования данных, арифметических вычислений и исполнения операций отношений в некриптографическом, но гомоморфном исполнении предлагается использовать классическую двоичную систему счисления в сочетании с системами счисления в остаточных классах (системы счисления *RNS*) и интервальной системой счисления.

СОК (Security Operation Center, SOC) основана на широко известной китайской теореме об остатках (Chinese Remainder Theorem, CRT). Она утверждает, что, зная наименьшие неотрицательные остатки от деления целого числа X на целые модули $m_1, m_2, \ldots, m_n$, возможно однозначно определить остаток от деления X на произведение этих модулей при условии, что модули попарно взаимно просты. СОК, в отличие от классических b-ичных систем счисления, задается не одним фиксированным основанием, а набором модулей $m_1, m_2, \ldots, m_n$ таких, что $gcd\left(m_i, m_j\right)=1$ для всех $i, j \in \{1,2,\ldots,n\}$, $i \neq j$, где $gcd()$ – наибольший общий делитель. Произведение этих модулей $M=\prod_{i=1}^{n} m_i$ определяет динамический диапазон СОК.

Целое число $X \in [0, M-1]$ представляется в виде вектора, составленного из наименьших неотрицательных остатков, получаемых при делении X на m_i:

$$X=\left(x_1, x_2, \ldots, x_n\right),$$

где $x_i = X \bmod m_i$, что также обозначается как $x_i = \left|X\right|m_i$.

Отрицательные числа также могут быть представлены в СОК. В общем случае, если X – это целое число со знаком, то диапазон возможных значений X, имеющих уникальное представление в СОК, определяется ограничением $-M \leqslant 2X < M$.

Над числами в СОК определены базовые операции, которые подразделяются на две группы. К операциям первой группы, которые иногда называют модульными, относятся сложение и вычитание чисел без возможности определения знака результата, умножение, а также деление без остатка (когда заранее известно, что делимое кратно делителю). Такие операции выполняются покомпонентно с остатками, без образования и учета переносов между ними. Пусть числа X, Y и Z представлены в виде

$$\left(x_1, x_2, \ldots, x_n\right),\ \left(y_1, y_2, \ldots, y_n\right) \text{ и } \left(z_1, z_2, \ldots, z_n\right)$$

соответственно. Тогда для всякой модульной операции ($\circ$) имеем

$$Z=\left(\left|x_1 \circ y_1\right|_{m1}, \left|x_2 \circ y_2\right|_{m2}, \ldots, \left|x_n \circ y_n\right|_{m_n}\right),$$

т.е. *i*-я цифра результата в СОК, $a\ z_i$, определяется значением $\left|x_i \circ y_i\right|_{m_i}$ | и не зависит ни от какой другой цифры z_j .

Это позволяет реализовать свободную от переносов параллельную компьютерную арифметику и делает СОК привлекательной системой счисления для использования в ресурсоемких приложениях, обеспечивает высокую надежность вычислений: ошибка в *i*-й цифре не оказывает влияния на другие цифры и поэтому может быть эффективно локализована и устранена.

Для операций второй группы, часто называемых немодульными, недостаточно знания значений отдельных остатков, а требуется оценка полной величины чисел: результат такой операции либо вообще не является числом в СОК, либо значение каждой его цифры (остатка) не является только лишь функцией значений соответствующих цифр операндов, а зависит от величины этих операндов.

К сожалению, непозиционная структура СОК не позволяет эффективно оценить величину числа по остаткам, и это обстоятельство является основным фактором, сдерживающим широкое распространение СОК в качестве альтернативы *b*-ичным системам счисления.

В работе [7] предложен метод сравнения чисел в СОК и выполнения связанных немодульных операций. Метод основан на идее, что не обязательно вычислять точное значение $\frac{X}{M}$, а достаточно иметь интервал $I\left(\frac{X}{M}\right)=\left[\frac{X}{M},\frac{X}{M}\right]$ такой, что $\frac{X}{M}\le\frac{X}{M}\le\frac{X}{M}$. Этот интервал называется интервальной оценкой с плавающей точкой числа *X* (или просто интервальной оценкой числа *X*).

Границы интервала – числа с плавающей точкой ограниченной разрядности. Вычисление $I\left(\frac{X}{M}\right)$ числа $X=(x_1,x_2,\ldots,x_n)$ выполняется в среднем за время $O(\log n)$ при распараллеливании на *n* потоков и требует только операций по модулям m_i и стандартных операций с плавающей точкой с направленными округлениями. Соответственно метод пригоден для современных вычислительных платформ общего назначения, которые поддерживают быструю арифметику IEEE 754.

Интервально-позиционная характеристика (ИПХ) по правилам интервальной арифметики принадлежит интервалу

$$I\left(\frac{X}{P}\right):=\left[\frac{X}{\underline{P}},\frac{\overline{X}}{P}\right]$$

с направленно округленными до ближайшего меньшего и ближайшего большего значений границами, которые удовлетворяют условию

$$\frac{X}{\underline{P}}\le E\left(\frac{X}{P}\right)\le\frac{\overline{X}}{P}.$$

ИПХ проецирует полный числовой диапазон *RNS* на полуинтервал [0, 1), сопоставляя всякое *RNS*-число *X* с парой округленных границ – позиционных чисел, которые локализуют относительную величину *X* [7].

Введем обозначения, которые будут использоваться в дальнейшем. Операции сложения и вычитания, умножения и деления над дробными числами, выполняемые с округлением к меньшему и большему представимому числу (аналогично операциям *toward*-∞ и *toward*+∞), будут, соответственно, обозначаться символами-операторами:

↑ – округление до ближайшего большего значения числа;

↓ – округление до ближайшего меньшего значения числа.

В том случае, если один из этих символов-операторов стоит перед групповым оператором, то все операции выполняются в соответствии с заданным типом округления.

Например, выражение $\uparrow(\sum_{i=1}^{n} x_i)$ означает, что все $(n-1)$ суммирования выполняются с округлением к большему.

Пусть в *RNS* с модулями $p_1, p_2, \ldots, p_n$ задано некоторое число $X = (x_1, x_2, \ldots, x_n)$. Для вычисления границ ИПХ справедливы формулы:

$$\underline{\frac{X}{P}} = \downarrow\left(\sum_{i=1}^{n} \left|(x_i)\cdot|P_i^{-1}\right| p_{p_i} | p_{p_i}\right), \tag{3}$$

$$\overline{\frac{X}{P}} = \uparrow\left(\sum_{i=1}^{n} \left|(x_i)\cdot|P_i^{-1}\right| p_{p_i} | p_{p_i}\right). \tag{4}$$

За счет направленных округлений возникающие погрешности приводят лишь к расширению ИПХ, оставляя отношение $E\left(\frac{X}{P}\right) \in I\left(\frac{X}{P}\right)$ истинным (существуют некоторые исключения, которые рассматриваются в дальнейшем). Это позволяет контролировать корректность результата выполнения немодульных операций путем анализа специальных признаков, указывающих на ситуации, когда точности ИПХ недостаточно для однозначной оценки $E\left(\frac{X}{P}\right)$.

Абсолютная ошибка ИПХ отражается в ее диаметре:

$$diamI\left(\frac{X}{P}\right) = \left(\overline{\frac{X}{P}}\right) - \left(\underline{\frac{X}{P}}\right). \tag{5}$$

Сложение и вычитание ИПХ задаются по аналогии с операциями над вещественными интервалами по правилам выполнения операций интервальной арифметики:

$$I\left(\frac{Z^+}{P}\right) = \left[\downarrow\left(\underline{\frac{X}{P}} + \underline{\frac{X}{P}}\right), \uparrow\left(\overline{\frac{X}{P}} + \overline{\frac{Y}{P}}\right)\right], \tag{6}$$

$$I\left(\frac{Z^-}{P}\right) = \left[\downarrow\left(\underline{\frac{X}{P}} - \overline{\frac{Y}{P}}\right), \uparrow\left(\overline{\frac{X}{P}} - \underline{\frac{Y}{P}}\right)\right]. \tag{7}$$

Для операций умножения и деления ИПХ справедливы аналогичные выражения и правила их выполнения.

Операция бинарного пересечения ИПХ определяется следующим образом:

$$I\left(\frac{X}{P}\right)\cap I\left(\frac{Y}{P}\right)=\left\{a\left|a\in I\left(\frac{X}{P}\right)\wedge a\in I\left(\frac{Y}{P}\right)\right.\right\}.$$

В терминах интервального анализа результат пересечения – это интервал:

$$\left[I\left(\frac{X}{P}\right)\cap I\left(\frac{Y}{P}\right)\right]=\left[\max\left\{\underline{\frac{X}{P}},\underline{\frac{Y}{P}}\right\},\min\left\{\overline{\frac{X}{P}},\overline{\frac{Y}{P}}\right\}\right].$$

Если $\operatorname{diam}\left[I\left(\frac{X}{P}\right)\cap I\left(\frac{Y}{P}\right)\right]\geq 0$, то $I\left(\frac{X}{P}\right)\cap I\left(\frac{Y}{P}\right)\neq\varnothing$, т.е. ИПХ пересекаются. Если же $\operatorname{diam}\left[I\left(\frac{X}{P}\right)\cap I\left(\frac{Y}{P}\right)\right]<0$, то ИПХ не пересекаются.

Если в качестве второго операнда выступает некоторое число c, эквивалентное вырожденному интервалу $[c]=[c,c]$, то непустое пересечение $I\left(\frac{X}{P}\right)\cap c$ равносильно включению $c\in I\left(\frac{X}{P}\right)$.

Очевидно, что если ИПХ чисел в *RNS* известны (ранее вычислены), то выполнение основных немодульных операций над ними становится тривиальным, поскольку сводится к анализу позиционных границ интервалов и оценке достоверности результата при соблюдении ряда формальных условий для получения корректного результата. Формальные условия корректности результата немодульной операции определяются согласно табл. 1.

Таблица 1

Условия корректного выполнения немодульных операций

Тип операции	Условие выполнения немодульной операции
Операция сравнения	$\operatorname{diam}\left[I\left(\frac{X}{P}\right)\cap I\left(\frac{Y}{P}\right)\right]<0$
Определение знака	$\operatorname{diam}\left[I\left(\frac{X}{P}\right)\cap I\left(\frac{P-1}{2P}\right)\right]<0\ \vee\ \overline{\frac{X}{P}}=\underline{\frac{P-1}{2P}}$
Контроль переполнения суммы	$\operatorname{diam}\left[I\left(\frac{Z^{+}}{P}\right)\cap 1\right]<0\vee\underline{\frac{Z^{+}}{P}}=1$
Контроль переполнения произведения	$\operatorname{diam}\left[I\left(\frac{Z^{\times}}{P}\right)\cap 1\right]<0\vee\underline{\frac{Z^{\times}}{P}}=1$

Результаты

Алгоритм гомоморфного выполнения операции сравнения двух чисел в RNS-системе счисления с использованием ИПХ

Для выполнения сравнения двух чисел при $X \neq Y$ необходимо выполнить следующие действия:

1. Вычислить ИПХ чисел X и Y:

$$I\left(\frac{X}{P}\right) \text{ и } I\left(\frac{Y}{P}\right).$$

2. Оценить *формальные условия* получения корректного результата.

3. При выполнении формальных условий корректности результата выполнить п. 4, иначе сформировать оповещение об ошибочном вычислении и завершить выполнение операции сравнения.

4. Определить результат, сопоставив ИПХ по правилам интервальной арифметики:

$$\text{если } \frac{X}{\underline{P}} > \frac{\overline{Y}}{P}, \text{ то } X > Y;$$

$$\text{если } \frac{\overline{X}}{P} < \frac{Y}{\underline{P}}, \text{ то } X < Y.$$

5. Завершить выполнение операции.

Например, требуется сравнить по величине числа $X = 1, 8, 7, 0$ и $Y = 6, 5, 10, 9$.

Рассмотрим выполнение этой операции сравнения:

1. Вычисляем ИПХ чисел X и Y с двумя значащими цифрами и значение диаметра результат:

$$\frac{X}{\underline{P}} = \downarrow |0,85 + 0,44 + 0,72 + 0,00|_1 = 0,01,$$

$$\frac{\overline{X}}{P} = \uparrow |0,86 + 0,45 + 0,73 + 0,00|_1 = 0,04,$$

$$\frac{Y}{\underline{P}} = \downarrow |0,14 + 0,77 + 0,18 + 0,92|_1 = 0,01,$$

$$\frac{\overline{Y}}{P} = \uparrow |0,15 + 0,78 + 0,19 + 0,93|_1 = 0,05.$$

2. Определяем диаметр интервала пересечения ИПХ:

$$\text{diam}\left[I\left(\frac{X}{P}\right) \cap I\left(\frac{Y}{P}\right)\right] = \min\left(\frac{\overline{X}}{P}, \frac{\overline{Y}}{P}\right) - \max\left(\frac{X}{\underline{P}}, \frac{Y}{\underline{P}}\right) = 0,04 - 0,01 > 0.$$

3. Оцениваем условия корректности выполнения операции сравнения. Условие не выполняются, так как интервалы ИПХ пересекаются и, значит,

при данной точности границ результат не может быть однозначно определен. Требуется повысить точность вычислений.

4. Вычислим ИПХ с тремя значащими цифрами:

$$\underline{\frac{X}{P}} = \downarrow |0,857 + 0,444 + 0,727 + 0,000|_1 = 0,028,$$

$$\overline{\frac{X}{P}} = \uparrow |0,858 + 0,445 + 0,738 + 0,00|_1 = 0,031,$$

$$\underline{\frac{Y}{P}} = \downarrow |0,14 + 0,77 + 0,18 + 0,92|_1 = 0,023,$$

$$\overline{\frac{Y}{P}} = \uparrow |0,15 + 0,78 + 0,19 + 0,93|_1 = 0,027.$$

В данном случае $\operatorname{diam}\left[I\left(\frac{X}{P}\right) \cap I\left(\frac{Y}{P}\right) \right] = -0,001$, поэтому сравнение будет выполнено корректно.

5. Выполняем сравнение ИПХ чисел. Так как $0,028 > 0,027$, то $X > Y$. Действительно, если перевести значения чисел из *RNS*-системы счисления в десятичную систему счисления, то $X = 260$, $Y = 230$ и отношение $X > Y$ верно.

Алгоритм гомоморфного выполнения операции определения знака числа в симметричных RNS-системах

В классических *RNS*-системах значения знаков чисел задаются неявно, из чего возникают сложности при выполнении арифметических операций. Для представления положительных и отрицательных чисел в симметричных *RNS*-системах при нечетном P диапазон $[0, P-1]$ разбивается на два интервала: $\left[0, \frac{P-1}{2}\right]$ и $\left[\frac{P+1}{2}, P-1\right]$. Первый интервал предназначен для представления положительных чисел, а второй – для представления отрицательных. При известном значении ИПХ числа для определения его знака достаточно сравнить $I\left(\frac{X}{P}\right)$ числа с ИПХ константы $I\left(\frac{P-1}{2P}\right)$, т.е. применить рассмотренный выше алгоритм выполнения операции сравнения.

Аналогично определяется знак результата выполнения арифметических операций. Ввиду тривиальности алгоритма определения знака числа его формальное описание не приводится.

Алгоритмы гомоморфной операции определения переполнения в RNS-системах счисления

При выполнении арифметических вычислений возможно возникновение ситуации, когда результат вычислений выходит за диапазон представления чисел, т.е. возникает переполнение. По правилам выполнения арифмети-

ческих операций в *RNS*-системах эта ситуация не контролируется и полученный результат воспринимается как правильный результат. При использовании ИПХ чисел контроль таких ситуаций возможен.

Рассмотрим выполнение операции сложения двух чисел X и Y: $Z^+ = X + Y$. Если X и Y имеют одинаковый знак, то процедура определения переполнения сводится к сопоставлению интервала-суммы с единицей: если $\frac{Z^+}{P} \geq 1$, то при суммировании произойдет переполнение, но если $\overline{\frac{Z^+}{P}} < 1$, то переполнение не произойдет (предполагается, что P – большое число и разницей между 1 и $\frac{P-1}{P}$ можно пренебречь). Признак переполнения при умножении двух модулярных чисел $Z^\times = X \times Y$ определяется аналогично. В контексте вычислительной математики метод интервальных оценок обладает следующими достоинствами:

1. Метод ориентирован на произвольно большие динамические диапазоны, не накладывает ограничений на набор модулей и их количество.

2. Алгоритмы вычисления $I\left(\frac{X}{M}\right)$ при равномерном распределении чисел-операндов имеют низкую вычислительную сложность и эффективно распараллеливаются.

3. Для вычисления $I\left(\frac{X}{M}\right)$ требуется выполнение только целочисленных операций и операций с плавающей точкой машинной точности.

Таким образом, применение предлагаемой ИПХ дает возможность выполнять немодульные операции непосредственно в формате системы СОК без преобразования численных данных в классический двоичный формат, т.е. в гомоморфном исполнении.

Алгоритмы гомоморфной арифметики в RNS-системах

Пусть многоразрядные числа x и y представлены как

$$x = s_x, X, I\left(\frac{X}{M}\right),\ y = s_y, Y, I\left(\frac{Y}{M}\right),$$

где $X = (x_1, x_2, \ldots, x_n)$ – модулярное представление числа X; $Y = (y_1, y_2, \ldots, y_n)$ – модулярное представление числа Y,

$$I\left(\frac{X}{M}\right) = \left[\downarrow I_l(X), \uparrow I_h(X)\right],\quad I\left(\frac{Y}{M}\right) = \left[\downarrow I_l(Y), \uparrow I_h(Y)\right],$$

s_x и s_y – знаки чисел.

Гомоморфные операции сложения, вычитания и умножения с такими числами просты в реализации даже с использованием современных аппаратных средств. На рис. 3 и 4 представлены алгоритмы сложения и вычитания чисел одинаковых знаков.

Алгоритм 1 $z \leftarrow x + y$

```
I(Z, M) ← I(X, M) + I(Y, M)                          ▷ Интервальная арифметика
if I_h(Z) ≤ I_l((M−1)/M) then
    s_z ← s_x
    for i ← 1, n do                                   ▷ Возможна параллельная обработка
        z_i ← (x_i + y_i) mod m_i
    end for
    return ⟨s_z, (z_1, z_2, ..., z_n), I(Z, M)⟩
else
    Обработка переполнения
end if
```

Рис. 3. Алгоритм гомоморфного сложения чисел одинаковых знаков в *RNS*

Алгоритм 2 $z \leftarrow x - y$

```
if X = Y then
    return 0
end if
if I_l(X) > I_h(Y) then                               ▷ X > Y
    s_z ← s_x
    for i ← 1, n do                                   ▷ Возможна параллельная обработка
        z_i = (x_i − y_i) mod m_i
    end for
    I(Z, M) ← I(X, M) − I(Y, M)
    return ⟨s_z, (z_1, z_2, ..., z_n), I(Z, M)⟩
else if I_h(X) < I_l(Y) then                          ▷ Y > X
    s_z ← −s_x
    for i ← 1, n do                                   ▷ Возможна параллельная обработка
        z_i = (y_i − x_i) mod m_i
    end for
    I(Z, M) ← I(Y, M) − I(X, M)
    return ⟨s_z, (z_1, z_2, ..., z_n), I(Z, M)⟩
else
    Уточнение знака
end if
```

Рис. 4. Алгоритм гомоморфного вычитания чисел одинаковых знаков

На рис. 5 представлен алгоритм умножения. Поскольку вычисления в СОК выполняются раздельно по каждому модулю, основные вычислительные циклы в этих алгоритмах могут быть эффективно распараллелены.

Алгоритм 3 $z \leftarrow xy$

```
I(Z/M) ← I(X/M) · I(Y/M)                              ▷ Интервальная арифметика
if I_h(Z) ≤ I_l((M−1)/M) then
    s_z ← s_x ⊕ s_y
    for i ← 1, n do                                   ▷ Возможна параллельная обработка
        z_i ← x_i y_i mod m_i
    end for
    return ⟨s_z, (z_1, z_2, ..., z_n), I(Z/M)⟩
else
    Обработка переполнения
end if
```

Рис. 5. Алгоритм гомоморфного умножения чисел в *RNS*

Представленные алгоритмы сложения и умножения реорганизованы таким образом, чтобы обеспечить возможность не только фиксации факта переполнения динамического диапазона, но и устранения переполнения посредством масштабирования либо расширения системы модулей СОК.

При вычитании чисел одинаковых знаков переполнения быть не может, однако возможна неоднозначность в определении знака результата ввиду недостаточной точности ИПХ. Для разрешения этой ситуации предлагается один из способов, описанных далее.

Способ 1. Выполнить повторное вычисление интервальной оценки с более высокой точностью. В этом случае $\left(\frac{X}{M}\right)$ и $\left(\frac{Y}{M}\right)$ вычисляются на основании остатков $(x_1, x_2, \ldots, x_n)$ и $(y_1, y_2, \ldots, y_n)$, после чего выполняется повторный вызов алгоритма вычитания.

Способ 2. Вычисляются представления чисел X и Y в системе счисления со смешанными основаниями (*mixed-radix system*), заданной основаниями $W_1 = 1$, $W_i = \prod_{j=1}^{i-1} m_j$ для $i = 2,3,\ldots,n$, где m_j – модули СОК.

Далее вычисленные представления $[\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n]$ и $[\overline{y}_1, \overline{y}_2, \ldots, \overline{y}_n]$ сравниваются поэлементно начиная со старших цифр $\overline{x}_n$ и $\overline{y}_n$. Если на i-й итерации сравнения оказывается $\overline{x}_i \neq \overline{y}_i$, то цикл сравнения завершается.

Деления на основе *RNS*-вычислений можно реализовать с использованием интервальных оценок делителя и делимого следующим образом.

Пусть $I\left(\frac{X}{M}\right) = \left[\downarrow \frac{X}{M}, \uparrow \frac{X}{M}\right]$ и $I\left(\frac{Y}{M}\right) = \left[\downarrow \frac{Y}{M}, \uparrow \frac{Y}{M}\right]$ – интервальные оценки делимого (остатка) X и делителя Y.

На каждой итерации алгоритма в арифметике с плавающей точкой вычисляется $q \leftarrow fl\nabla\left(\frac{X}{M} \div \frac{Y}{M}\right)$, где $fl\nabla$ означает, что вычисления внутри скобок выполняются с округлением «вниз» (к минус бесконечности).

Поскольку q – число с плавающей точкой, оно имеет вид $q = f \times 2^e$, причем $I\left(\frac{X}{M}\right) = [1 \le f < 2]$. Значение e используется в качестве адреса подстановочной таблицы для выбора очередного приближения частного:

$$Qi = \left|2^e\right|_{m1}, \left|2^e\right|_{m2}, \ldots, \left|2^e\right|_{mn},$$

после чего остаток X корректируется и $I\left(\frac{X}{M}\right)$ вычисляется вновь. Итерации продолжаются до тех пор, пока $\left(\frac{X}{M}\right) \ge I\left(\frac{Y}{M}\right)$. Таким образом, деление требует только операций по небольшим модулям m_i и стандартных операций с плавающей точкой. В редких случаях после основного цикла может возникнуть неоднозначность, которая устраняется вызовом *MRC*-алгоритма.

Обсуждение

Перспективен переход к активному использованию нейросетевых декомпозиций при интерпретации решающих правил искусственного интеллекта с использованием рассмотренных методов выполнения арифметических вычислений в *RNS* с использованием интервально-позиционных характеристик операндов.

Примером могут служить приложения нейросетевой биометрии. Так, лица людей сегодня анализируются многослойными нейросетями глубокого обучения [1, 2], а слитная речь людей анализируется лингвистическими нейросетевыми архитектурами голосовых помощников.

Примерно та же самая ситуация возникает и при анализе рукописных парольных фраз. На рис. 6 представлена общая схема работы среды моделирования БиоНейроАвтограф [8, 9], используемой в Пензенском государственном университете с 2012 г. для самостоятельного выполнения лабораторных работ студентами кафедры «Информационная безопасность систем и технологий».

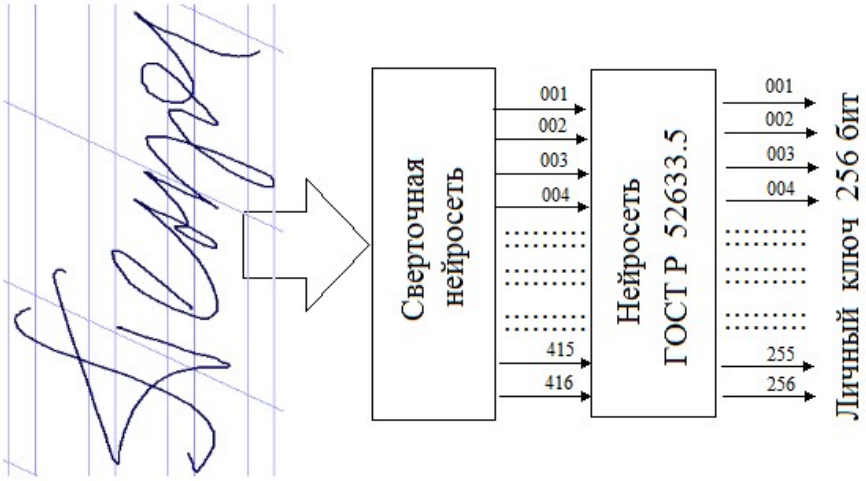

Рис. 6. Нейросетевое преобразование рукописного пароля в код личного ключа

Из рис. 6 видно, что биометрические данные рукописного пароля «*Пенза*» сверточная нейросеть преобразует в вектор из 416 биометрических параметров, которые вторая нейросеть, обученная по ГОСТ Р 52633.5–2011[1] преобразует в личный ключ пользователя длиной 256 бит.

Алгоритм обучения по ГОСТ Р 52633.5–2011 ориентирован на архитектуру однослойной нейросети, у которой каждый из нейронов отвечает за один бит выходного ключа. При этом нейрон имеет линейный обогатитель входной и относительно бедной биометрической информации вектора из 416 параметров. Для каждого пользователя формируется собственная архитектура нейросети через случайный выбор из 24 биометрического параметров для каждого из 256 искусственных нейронов.

[1] ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

В свою очередь любой из нейронов имеет выходной бинарный квантователь, сравнивающий обогащенные данные с порогом 0,0. В итоге мы получаем описание нейрона системой из трех соотношений:

$$\begin{cases} y = a_0 + \sum_{i=1}^{24} a_i \cdot x_i, \\ z = 0, \quad if \quad y < 0, \\ z = 1, \quad if \; y > 0. \end{cases} \tag{14}$$

Следует обратить внимание на то, что отклики нейрона всегда дискретны, это помечено кавычками, тогда как входные переменные и весовые коэффициенты континуальны. Принципиально важно, что используются только операции сложения «+», умножения «×», сравнения и численные значения нейрона кодируются 8-разрядным двоичным кодом.

В итоге можно гомоморфно зашифровать 8-разрядные данные нейрона и отправить их в «облако» для вычисления отклика входного накопителя данных искусственного нейрона. Если выполнять гомоморфное шифрование по стандарту ISO/IEC 18033-6 на некотором ключе длиной 1024 бита, то после защищенных «облачных» вычислений мы получим отклик в неизвестном масштабе. Восстановить верный масштаб данных и настройку порога может владелец информации, обладающий ключом гомоморфного расшифровывания.

Преимуществом декомпозиции любого решающего правила ИИ в виде нейросети из 256 искусственных нейронов является то, что каждый линейный обогатитель входной биометрической информации каждого из нейронов уже является суперпозицией операций сложения и умножения. То есть входные накопители информации персептронов уже являются естественными конструкциями, удобными для сокрытия внешних вычислений в недоверенной среде механизмами гомоморфного шифрования.

Еще одним преимуществом нейросетевой декомпозиции решающих правил ИИ является то, что линейные накопители устойчивы. При суммировании незначительные ошибки 8-разрядных представлений входных данных и весовых коэффициентов усредняются. Если во внешней недоверенной вычислительной среде вычислять только состояния линейных накопителей, то ошибки при гомоморфных вычислениях не накапливаются. Снимается одна из проблем международного стандарта ISO/IEC 18033-6, исчезает эффект накопления ошибок. Остается только проблема высокого потребления энергии при гомоморфном шифровании/расшифровывания данных алгоритмами RSA с длинными числами.

Добиться многократного снижения энергозатрат на сокрытие информации удается, если отказаться от использования асимметричной криптографии длинных чисел. Такая возможность появляется, если перейти к гомоморфному маскированию содержания вычислений в неопределенной для внешнего наблюдателя системе остаточных классов [3, 10].

Заключение

Показано, что для защиты ИИ в нейросетевом исполнении успешно можно использовать гомоморфные *RNS*-вычисления с использованием ин-

тервально-позиционных характеристик значений нейронов. Такой подход позволяет защитить ИИ от несанкционированных воздействий из вне, так как внешнему несертифицированному пользователю необходимо знать значения, количество и порядок использования модулей систем *RNS*. Последнее является нетривиальной задачей и требует выполнять комбинаторный перебор в поле простых чисел. Кроме этого, существенно повышается скорость обработки по сравнению с криптографическими методами защиты систем ИИ за счет параллельной обработки знаков чисел (значений) нейронов, снижается энергоемкость и техническая сложность реализации аппаратных решений ввиду использования малоразрядных операндов. В итоге изложенный подход представляется перспективным для нейросетевых систем ИИ.

Сегодня на базе некриптографических преобразований *RNS* с низким энергопотреблением могут производиться доверенные контроллеры низкой стоимости в рамках *RNS*-поддержки гомоморфной по отношению к двум типам операций: операциям сложения «+» и операциям умножения «×».

Принципиально важно, что перечень операций, для которых *RNS*-преобразования позволяют добиться гомоморфизма, может быть расширен с 2 до 6 (см. табл. 1), можно существенно расширить перечень защищаемых от исследования нейросетевых архитектур.

Список литературы

1. Николенко С., Кудрин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб. : Изд.-дом «Питер», 2018.
2. Аггарвал Чару. Нейронные сети и глубокое обучение. СПб. : Диалектика, 2020. 756 с.
3. Князьков В. С., Исупов К. С., Иванов А. И., Артемов И. И. Гибридные вычисления и их применение для построения гомоморфных нейросетевых систем доверенного искусственного интеллекта // Наука, общество, технологии: проблемы и перспективы взаимодействия в современном мире. Петрозаводск : МЦНП «Новая наука», 2022. С. 5–65. doi: 10.46916/30062022-978-5-00174-630-0
4. Kairouz P., McMahan H. B., Bellet A. [et al.]. Advances and Open Problems in Federated Learning // Foundations and Trends in Machine Learning. 2021. Vol. 14, № 1. doi: 10.1561/2200000083 URL: https://www.nowpublishers.com/article/Details/MAL-083 (дата обращения: 07.04.2021).
5. Qi Xia, Winson Ye, Zeyi Tao, Jindi Wu, Qun Li. A Survey of Federated Learning for Edge Computing: Research Problems and Solutions // High-Confidence Computing. 2021. doi: 10.1016/j.hcc.2021.100008 URL: https://www.sciencedirect.com/science/article/pii/S266729522100009X. (дата обращения: 07.04.2021).
6. Choudhury O., Gkoulalas-Divanis A., Salonidis T., Sylla I., Park Y., Hsu G., Das A. Differential privacy-enabled federated learning for sensitive health data // ARXIV.ORG. URL: https://arxiv.org/abs/1910.02578 (дата обращения: 07.04.2021).
7. Isupov K., Knyazkov V. Interval estimation of relative values in residue number system // Journal of Circuits, Systems and Computers. 2018. Vol. 27, № 1. P. 1850004. doi: 10.1142/S02181266
8. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» [Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»]. URL: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip
9. Иванов А. И. Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях : учеб. пособие. Пенза, 2013. 30 с. URL: http://пниэи.рф/activity/science/noc/tm_IvanovAI.pdf

10. Князьков В. С., Иванов А. И., Безяев А. В., Лукин В. С. Бескомпроматное привлечение сторонних ресурсов низкого доверия для выполнения вычислений высокого доверия в SIM-картах и микро SD-картах с защитой персональных биометрических данных нейро-гомоморфным шифрованием // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 55–62.

References

1. Nikolenko S., Kudrin A., Arkhangel'skaya E. *Glubokoe obuchenie. Pogruzhenie v mir neyronnykh setey = Deep learning: a dive into the world of neural networks*. Saint Petersburg: Izd.-dom «Piter», 2018. (In Russ.)
2. Aggarval Charu. *Neyronnye seti i glubokoe obuchenie = Neural Networks and Deep Learning.* Saint Petersburg: Dialektika, 2020:756. (In Russ.)
3. Knyaz'kov V.S., Isupov K.S., Ivanov A.I., Artemov I.I. Hybrid computing and its application to building homomorphic neural network systems of trusted artificial intelligence. *Nauka, obshchestvo, tekhnologii: problemy i perspektivy vzaimodeystviya v sovremennom mire = Science, society, technology: problems and prospects of interaction in the modern world*. Petrozavodsk: MTsNP «Novaya nauka», 2022:5–65. (In Russ.). doi: 10.46916/30062022-978-5-00174-630-0
4. Kairouz P., McMahan H.B., Bellet A. et al. Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*. 2021;14(1). (In Russ.). doi: 10.1561/2200000083 Available at: https://www.nowpublishers.com/article/Details/MAL-083 (accessed 07.04.2021).
5. Qi Xia, Winson Ye, Zeyi Tao, Jindi Wu, Qun Li. A Survey of Federated Learning for Edge Computing: Research Problems and Solutions. *High-Confidence Computing*. 2021. doi: 10.1016/j.hcc.2021.100008 Available at: https://www.sciencedirect.com/science/article/pii/S266729522100009X. (accessed 07.04.2021).
6. Choudhury O., Gkoulalas-Divanis A., Salonidis T., Sylla I., Park Y., Hsu G., Das A. Differential privacy-enabled federated learning for sensitive health data. *ARXIV.ORG*. Available at: https://arxiv.org/abs/1910.02578 (accessed 07.04.2021).
7. Isupov K., Knyazkov V. Interval estimation of relative values in residue number system. *Journal of Circuits, Systems and Computers*. 2018;27(1):1850004. doi: 10.1142/S02181266
8. Ivanov A.I., Zakharov O.S. *Sreda modelirovaniya «BioNeyroAvtograf». [Programmnyy produkt sozdan laboratoriey biometricheskikh i neyrosetevykh tekhnologiy, razmeshchen s 2009 g. na sayte AO «PNIEI»] = Modeling environment "BioNeyroAvtograf". [The software product was created by the laboratory of biometric and neural network technologies and has been posted on the website of JSC PNIEI since 2009.]*. Available at: http://pniei.rf/activity/science/noc/bioneuroautograph.zip
9. Ivanov A.I. *Avtomaticheskoe obuchenie bol'shikh iskusstvennykh neyronnykh setey v biometricheskikh prilozheniyakh: ucheb. posobie = Automatic training of large artificial neural networks in biometric applications: textbook.* Penza, 2013:30. (In Russ.). Available at: http://pniei.rf/activity/science/noc/tm_IvanovAI.pdf
10. Knyaz'kov V.S., Ivanov A.I., Bezyaev A.V., Lukin V.S. Uncompromising access to third-party low-trust resources to achieve high-trust calculations in SIM cards and microSD cards with neuromorphic encryption of protected personal biometric data. *Bezopasnost' informatsionnykh tekhnologiy: sb. nauch. st. po materialam III Vseros. nauch.-tekhn. konf.: v 2 t. = Information Technology Security: proceedings of the 3rd All-Russian scientific and engineering conference: in 2 volumes.* Penza: Izd-vo PGU, 2021;1:55–62. (In Russ.)

Информация об авторах / Information about the authors

Владимир Сергеевич Князьков
доктор технических наук, профессор, главный научный сотрудник Научно-исследовательского института фундаментальных и прикладных исследований, Пензенский государственный университет (Россия, г. Пенза, ул. Красная, 40)

E-mail: kniazkov@list.ru

Vladimir S. Knyazkov
Doctor of engineering sciences, professor, principal researcher of the Research Institute of Fundamental and Applied Research, Penza State University (40 Krasnaya street, Penza, Russia)

Александр Иванович Иванов
доктор технических наук, профессор, научный консультант, Пензенский научно-исследовательский электротехнический институт (Россия, г. Пенза, ул. Советская, 9)

E-mail: ivan@pniei.penza.ru

Aleksandr I. Ivanov
Doctor of engineering sciences, professor, scientific adviser, Penza Scientific Research Electrotechnical Institute (9 Sovetskaya street, Penza, Russia)

Константин Сергеевич Исупов
кандидат технических наук, доцент, доцент кафедры электронных вычислительных машин, Вятский государственный университет (Россия, г. Киров, ул. Московская, 36)

E-mail: isupov.k.s.work@gmail.com

Konstantin S. Isupov
Candidate of engineering sciences, associate professor, associate professor of the sub-department of electronic computers, Vyatka State University (36 Moskovskaya street, Kirov, Russia)

Михаил Матвеевич Бутаев
доктор технических наук, профессор, ученый секретарь, Научно-производственное предприятие «Рубин» (Россия, Пенза, ул. Байдукова, 2)

E-mail: isupov.k.s.work@gmail.com

Mikhail M. Butayev
Doctor of engineering sciences, professor, scientific secretary, Research and Production Enterprise “Rubin” (2 Baydukova street, Penza, Russia)

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflicts of interests.

Поступила в редакцию / Received 15.10.2024

Поступила после рецензирования и доработки / Revised 08.11.2024

Принята к публикации / Accepted 12.12.2024