Дата поступления рукописи в редакцию: 21.05.2026 г.
Дата принятия рукописи в печать: 02.06.2026 г.
DOI: 10.24412/2782-3830-2026-5-306-313

СЕМЕНОВ Александр Александрович,
научный сотрудник ФКУ НПО «СТиС» МВД России,
e-mail: mail@law-books.ru

АВЕТИСЯН Карэн Рафаелович,
Старший преподаватель кафедры
информационных технологий и организации
расследования киберпреступлений
Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева,
e-mail: Karen-Avetisyan-1989@bk.ru

ОРГАНИЗАЦИОННЫЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИЙ

Аннотация. *В статье рассматриваются особенности внедрения искусственного интеллекта в организациях, включая выбор задач, работу с данными и вопросы безопасности. Подчеркивается необходимость поэтапного внедрения нейросетей и корректной подготовки обучающих данных. Анализируются риски, связанные с конфиденциальностью, уязвимостями и адверсариальными атаками, а также вопросы оценки эффективности и ресурсного обеспечения.*

Ключевые слова: *искусственный интеллект, внедрение ИИ, нейросети, машинное обучение, датасеты, конфиденциальность данных, адверсариальные атаки, безопасность, вычислительные ресурсы, оптимизация затрат.*

SEMENOV Aleksandr Aleksandrovich,
Chief Researcher, Federal State Budgetary Institution "STIS"
of the Ministry of Internal Affairs of the Russian Federation

AVETISYAN Karen Rafaelovich,
Senior Lecturer, Department of Information
Technology and Cybercrime Investigation Organization
Moscow Academy of the Investigative Committee
of the Russian Federation named after A. Ya. Sukharev

ORGANIZATIONAL AND PRACTICAL ASPECTS OF IMPLEMENTING ARTIFICIAL INTELLIGENCE IN ORGANIZATIONS

Annotation. *This article examines the specifics of implementing artificial intelligence in organizations, including task selection, data management, and security issues. It emphasizes the need for a phased implementation of neural networks and the correct preparation of training data. Risks associated with privacy, vulnerabilities, and adversarial attacks are analyzed, as well as issues of performance assessment and resource provision.*

Key words: *artificial intelligence, AI implementation, neural networks, machine learning, datasets, data privacy, adversarial attacks, security, computing resources, cost optimization.*

Рассмотрим организационные аспекты применения искусственного интеллекта, т. е. его внедрение в различные сферы деятельности.

Машинное обучение развивается децентрализовано экспериментальным путем и направлять процесс его развития бессмысленно. Эти утверждения будто бы оказываются в противоре-

чии с тем, что последние годы крупные зарубежные и отечественные компании тратят существенные суммы на обучение больших языковых моделей. Обучение этих нейросетей требует затрат огромных ресурсов и, следовательно, по определению доступно только большим компаниям или государственным учреждениям. Однако надо видеть разницу между хаотичным появлением новых подходов и направленным развитием тех из них, которые показали свою эффективность. Другими словами:

Если изобретение новых типов нейросетей едва ли поддается управлению, то освоение уже придуманных – вполне направляемый процесс.

Соответственно, под внедрением искусственного интеллекта следует понимать освоение уже разработанных методов и подходов машинного обучения и практическое применение соответствующих нейросетей.

Машинное обучение – слишком широкая область знаний, не направленная на какую-то конкретную практическую задачу или область как, например, ядерная физика может быть направлена на развитие энергетики, генная инженерия – на лечение болезней и т. д. Вместе с тем представление об искусственном интеллекте непрофильного специалиста сильно засорено влиянием темы нейроморфных вычислений и другими общефилософскими соображениями. В результате широко распространено ошибочное представление о том, что искусственный интеллект – это некоторая разумная сущность, способная решать произвольные задачи. Как следствие, при постановке задачи внедрения искусственного интеллекта в некоторое крупное учреждение или компанию зачастую часто представляют себе объект внедрения как некоторую многофункциональную систему, в которой искусственный интеллект должен занять место в голове (*рисунок 1, слева*).

Рисунок 1. Объект внедрения как некоторая многофункциональная система

В действительности, разумеется, должно происходить наоборот: искусственный интеллект реализуется в виде отдельных нейросетей, каждая из которых выполняет свою элементарную функцию где-то в системе (рисунок 1, справа). Некоторая сложность осознания этой конструкции заключается в том, что возможность применения искусственного интеллекта для совершенствования конкретных функций возникает чаще всего не в тех подразделениях, где есть специалисты по искусственному интеллекту, и, напротив, специалисты по искусственному интеллекту в некоторой организации могут не иметь представления о конкретных прикладных задачах, решаемых другими сотрудниками организации.

Внедрение искусственного интеллекта в крупной организации должно происходить снизу вверх путем определения из числа элементарных практических задач, возникающих на местах тех задач, которые в настоящее время могут эффективно решаться с помощью нейросетей, и постепенного внедрения соответствующих нейросетей для решения этих отдельных задач.

Для решения каждой отдельной задачи нужен датасет. Подготовка датасета необходимого объема может быть трудоемкой, но гораздо чаще проблема заключается не в разметке, а в доступе к данным как таковым. В особенности остро проблема стоит в ситуациях, когда эти данные являются конфиденциальными. Понимание того, что создание нейросетей требует наличия обучающих данных, не распространено повсеместно, поэтому конфиденциальность данных часто оказывается непреодолимым препятствием. В связи с этим распространены попытки создать нейросеть, выполняющую целевую задачу на смоделированных данных, сильно или даже до неузнаваемости отличающихся от реальных.

Обучение нейросетей на искусственных/модельных/ синтетических данных с дальнейшим инференсом на реальных данных работает в редчайших случаях, в большинстве же случаев обученная нейросеть не будет работать.

Для преодоления ограничений конфиденциальности в некоторых случаях доступны следующие приемы:

1) из конфиденциальных данных можно извлечь только необходимую для обучения нейросети информацию, а остальную либо совершенно не использовать, либо заменить на безликие номера;
2) процесс обучения нейросети можно выполнить по месту хранения конфиденциальных данных, при необходимости даже без подключения к интернету;
3) можно осуществить частичную обработку конфиденциальных данных с помощью нескольких первых слоев нейросети, обученной на не конфиденциальных данных, после чего передать полученные значения для дальнейшего обучения оставшейся части нейросети.

В общем случае обучающий датасет должен состоять строго точно из таких же данных, которые будут подаваться в нейросеть в инференсе, и никак иначе.

Например, первый прием часто используется в медицине для обучения нейросетей-помощников, при этом специалисты по машинному обучению не знают, кому принадлежат конкретные медицинские сведения.

Еще одним вопросом в контексте безопасности является мыслимая способность самой нейросети по собственной воле нанести какой-то урон, например, передать секретные данные или даже занести компьютерный вирус.

Причиной этих заблуждений чаще всего является то, что нейросети и искусственный интеллект мысленно приравнивают к компьютерным программам и, соответственно, приписывают им те же уязвимости. Как мы знаем, нейросеть – это алгоритм, чаще всего описанный в некотором файле с известным форматом. В любом случае, нейросеть не может ничего сделать самостоятельно без фреймворка или библиотеки, исполняющих вычисления этой нейросети. Фреймворки и библиотеки уже являются программным обеспечением, рассмотрение вопроса наличия в них уязвимостей теоретически имеет смысл. Однако на практике чаще всего исполь-

зуют широко распространенные фреймворки и библиотеки, зачастую с открытым исходным кодом. Вероятность наличия уязвимостей в таком программном обеспечении невелика, а вероятность наличия намеренно заложенных уязвимостей совершенно ничтожна. Если, однако, требуется стопроцентная уверенность в безопасности программного обеспечения, то без особого труда можно выполнить соответствующие проверки используемых фреймворков и библиотек также, как и для любого другого программного обеспечения.

Нейросети не могут содержать программных уязвимостей, их теоретически могут содержать только программные средства, используемые для обучения и инференса нейросетей, что маловероятно.

С обработкой конфиденциальной информации связан также мыслимый риск ее извлечения из нейросети. Такого рода опасения могут иметь место только в части случаев. Например, сверточная нейросеть, выполняющая детекцию объектов на видео, при обучении обобщила весь увиденный датасет в несколько мегабайт данных, из которых совершенно невозможно извлечь хоть какую-то единицу оригинальной информации. Напротив, трансформер декодерного типа, который при обучении ознакомился с текстом конфиденциального содержания, может содержать фрагмент исходной информации в закодированном виде и выдать его при диалоге с пользователем.

Не из всех нейросетей возможно извлечь исходную конфиденциальную информацию, использованную при обучении.

Ложно также представление о том, что программное обеспечение может умышленно заложить в нейросеть какой-нибудь недостаток, например, что нейросеть, обученная распознавать военную технику с помощью вредоносного фреймворка, не будет в инференсе распознавать технику определенной страны. Гипотетическое закладывание злоумышленником таких свойств в нейросеть, обучаемую неизвестным человеком на неопределенном заранее датасете, невозможно, теоретически оно возможно только через закладывание особенностей в датасет. С другой стороны, знание разработчиком происхождения датасета и понимание используемого формата описания нейросети, строения составляющих ее слоев и параметров процесса машинного обучения дают ему полное представление о том, какие данные из датасета и как закладываются в нейросеть и, следовательно, исключают возможность постороннего вмешательства.

При этом, даже если из нейросети нельзя извлечь конфиденциальную информацию, использованную при обучении, само по себе описание нейросети вместе со значениями весов может составлять существенный интерес для врага или злоумышленника. В самом простом случае полное описание нейросети может составлять коммерческую ценность или давать представление о тактико-технических характеристиках устройств и систем, использующих эту нейросеть. Кроме того, существуют способы нахождения уязвимостей нейросетей.

Адверсариал атака/adversarial attack – процесс нахождения особенностей входных данных нейросети, к которым нейросеть особенно чувствительна и изменение которых может резко изменить точность ее работы.

Принцип адверсариал атак следующий: у нейросети фиксируют веса, а в качестве весов воспринимают значения входных данных. При этом градиентный спуск выполняют как бы в обратную сторону, т. е. пытаются так изменить входные данные, чтобы ошибка работы нейро-

сети была максимизирована. Обнаружено, например, что даже очень качественно обученные сверточные нейросети могут давать диаметрально противоположные результаты на двух изображениях, отличающихся несколькими пикселями. Наиболее продвинутые методы в этой области позволяют находить устойчивые паттерны, которые при попадании в состав входных данных делают нейросеть совершенно неработоспособной. Так, например, есть ряд работ, где разработчики придумали рисунок для футболки, из-за которого нейросеть становится неспособной распознать человека или его лицо (*рисунок 2*).

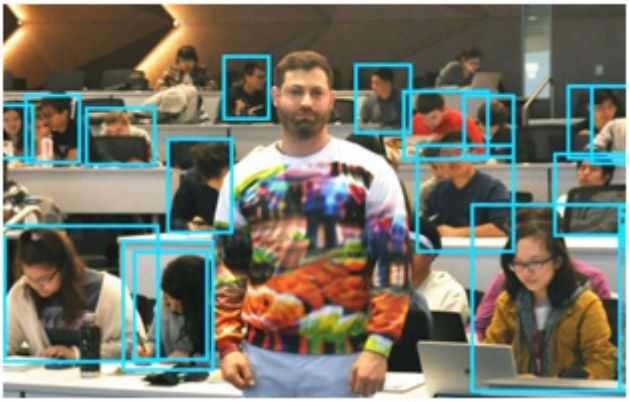

Рисунок 2. Нейросеть распознает человека и его лицо.

Можно представить себе применение адверсариал атаки к нейросети, извлеченной из образца военной или специальной техники, для создания камуфляжа. Отсюда прогнозируется, что в ближайшем будущем в области безопасности нейросетей будут развиваться параллельно как способы атаки (т. е. нахождения уязвимостей нейросетей), так и способы защиты (т. е. способов обучения нейросетей, устойчивых к атакам).

Попадание описания обученной нейросети в руки злоумышленника дает ему теоретическую возможность нейтрализовать действие нейросети.

Еще одним распространенным заблуждением является идея о том, что нет способа оценить качество работы нейросети, нейросеть работает непредсказуемо и т. д. Такого рода опасения имеют корни в непонимании природы нейросетей. В действительности нейросети зачастую выполняют задачи, функционально аналогичные тем, что раньше выполнялись традиционными алгоритмами, и к ним, соответственно, применяют те же метрики качестве что и к традиционным алгоритмам. Например, точность машинного перевода рекуррентными нейросетями текстов с языка на язык оценивается теми же способами, что и для алгоритмов предыдущих поколений. Тем не менее, на практике часто возникает позыв дать человекоподобное объяснение результату работы нейросети, грубо говоря, спросить у нее: «почему ты сделала так, а не так?». Разумеется, с уже обученной нейросетью такое сделать невозможно, однако в редких случаях удается создать нейросеть, которая в процессе своей работы создает промежуточную информацию, частично объясняющую логику ее работы.

Машинное обучение по определению создает алгоритм, который человек не был способен сам создать и, следовательно, едва ли может объяснить логику его работы. По этой причине в общем случае объяснимость логики работы нейросети недостижима, стремление к приданию результатам работы нейросети объяснимости может только ухудшить качество конечного результата.

В силу того, что машинное обучение в современном его понимании является совершенно новой областью знаний, среди специалистов по нему абсолютно подавляющее большинство составляют молодые люди до 30–35 лет. Конечно, встречаются исключения, однако в среднем в настоящее время от коллектива специалистов по искусственному интеллекту следует ожидать, что он будет состоять преимущественно из людей младшей возрастной категории. Спрос на этих специалистов стабильно растет, в основном со стороны преуспевающих коммерческих компаний. Соответственно, ожидания от уровня зарплаты и условий труда у таких специалистов несколько завышены, в связи с чем длительное время содержать подобный коллектив может быть затруднительно. Для крупных ведомств и организаций, решающих научно-технические задачи, целесообразно содержать небольшое количество профильных специалистов в этой области для решения ими части задач и постановки других задач внешним организациям. Освоение машинного обучения непрофильными специалистами, уже находящимися в штате организации, может значительно повысить их возможности на рынке труда и, таким образом, привести к потере организацией ценных сотрудников.

Аппаратное обеспечение разработки или эксплуатации нейросетей зачастую оказывается даже дороже, чем оплата труда специалистов. При оценке необходимых вычислительных ресурсов следует четко разделять стадии машинного обучения и инференса, а зависимости от постановки решаемой задачи требования к оборудованию на них могут кардинально отличаться. Важным аспектом выбора оборудования должно быть наличие поддерживающих это оборудование фреймворков и/или библиотек, так как создание подобных собственным силами требует привлечения специалистов по низкоуровневой оптимизации программ (которых еще меньше, чем специалистов по машинному обучению) и может занять существенное время.

Выбор моделей, объема и конфигурации оборудования должен исходить из оценки объема выполняемых вычислений и срока, в течение которого эти вычисления выполняются. Ориентироваться при этом на номинальные значения производительности во флопсах, указываемые поставщиком оборудования, нельзя, так как на практике эффективность использования оборудования сильно зависит от конкретной задачи и часто в несколько раз ниже 100 %. Кроме того, распараллеливание вычислений чаще всего нетривиально, поэтому нельзя вычислять мощность некоторого вычислительного оборудования просто как сумму слагаемых, в него входящих.

Оценка требуемого для выполнения машинного обучения или эксплуатации нейросетей вычислительного оборудования и соответствующих затрат чрезвычайно важна.

Правильнее всего выполнить самостоятельно или найти данные о тестах производительности, выполненных в схожих условиях (обучение или инференс, похожая архитектура нейросети, близкие размеры входных данных, не во многие разы отличающиеся размеры батча), и сделать соответствующие оценки, аккуратно разобравшись с используемыми единицами исчисления и табличными значениями характеристик видеокарт. К этому следует относиться особенно внимательно при оценке стоимости работ, выполняемых сторонней организацией по заказу, поскольку в данном вопросе существует огромный соблазн выполнить оценку поверхностно «сверху», выбрать оборудование подороже или еще как-нибудь перестраховаться.

Если заказчик работ не выполняет такую оценку или не ознакамливается с оценкой, выполненной исполнителем работы, то можно ожидать, что объем средств, затрачиваемых на вычислительной оборудование, в несколько раз превзойдет необходимый.

Кроме закупки оборудования существует еще опция его аренды. При аренде оборудования одним из ключевых вопросов становится степень его загрузки полезной работой. Наиболее выгодные предложения и тарифы на аренду вычислительного оборудования предоставляются исходя из расчета, что покупатель использует оборудование круглосуточно (подобно тому, как аренда

гаража оплачивается за календарный период вне зависимости от того, стоит в гараже автомобиль или нет). Соответственно, аренда оборудования и загрузка его вычислениями раз в несколько дней фактически эквивалентна переплате в несколько раз. Как правило, арендодатели закладывают такие цены, чтобы оборудование окупало себя за один-два года, соответственно аренда оборудования в течение года или более длительного срока вполне вероятно окажется дороже, чем закупка точно такого же оборудования и его самостоятельная эксплуатация.

Список литературы:

[1] Chen Zhang, Joohee Kim Video object detection with two-path convolutional LSTM pyramid. 2016. – URL: https://www.researchgate.net/publication /343702579_Video_Object_Detection_With_ Two-Path_ Convolutional_LSTM_ Pyramid/fulltext/5f3b2658928 51cd302013482/Video-Object-Detection-With-Two-Path-Convolutional-LSTM-Pyramid.pdf/ (дата обращения: 16.01.2026).

[2] Hanson A., Koutilya PNVR, Sanjukta Krishnagopal, Larry Davis Bidirectional Convolutional LSTM for the Detection of Violence in Videos. 2018. – URL: https://openaccess.thecvf.com/content_eccv_2018_workshops/w10 /html/Hanson_Bidirectional_Convolutional_LSTM_or_the_ Detection_of_Violence_in_ Videos_ ECCVW_2018_paper.html (дата обращения: 15.01.2026).

[3] Howard A.G., Menglong Zhu, Bo Chen, Kalenichenko D. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. 2017. – URL: https://arxiv.org/pdf/1704.04861/ (дата обращения: 11.01.2026).

[4] Iandola F.N., Han S., Moskewicz M.W., Ashraf K., Dally W.J., Keutzer K. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size Recognition. 2016. Published as a conference paper at ICLR. 2015. – URL: https://www. researchgate.net/publication/ 301878495_SqueezeNet_AlexNet-level_accuracy_ with_50x_fewer_ parameters_ and_05MB_model_size (дата обращения: 10.01.2026).

[5] Ioffe S., Szegedy C. Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. 2015. – URL: https://arxiv.org/pdf/1502.03167/ (дата обращения: 13.01.2026).

[6] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun Deep Residual Learning for Image Recognition. 2015. – URL: https://arxiv.org/pdf/1512.03385 (дата обращения: 11.01.2026).

[7] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun Spatial pyramid pooling in deep convolutional networks for visual recognition. 2015. – URL: https://arxiv.org/pdf/1406.4729/ (дата обращения: 11.01.2026).

[8] Krizhevsky I., Sutskever I., Hinton G.E. Imagenet classification with deep convolutional neural networks. 2012. – URL: https://proceedings.neurips.cc/paper_files/paper/2012/file/c399862d3b9d6b76c8436e 924a68c45b-Paper.pdf (дата обращения: 12.01.2026).

[9] Lavin A., Scott Gray Fast Algorithms for Convolutional Neural Networks. 2015. – URL: https://arxiv.org/abs/1509.09308 (дата обращения: 11.01.2026).

[10] Mikolov T., Kai Chen, Corrado G., Jeffrey Dean Efficient Estimation of Word Representations in Vector Space. 2013. – URL: https://arxiv.org/abs/1301.3781 (дата обращения: 15.01.2026).

[11] Norman P. Jouppi, Cliff Young, Nishant Patil and others In-Datacenter Performance Analysis of a Tensor Processing Unit. 2017. – URL: https://arxiv.org/pdf/1704.04760 (дата обращения: 11.01.2026).

[12] Ronneberger O., Fischer Ph., Brox Th. U-Net: Convolutional Networks for Biomedical Image Segmentation. 2015. – URL: https://arxiv.org/pdf/1505.04597/ (дата обращения: 13.01.2026).

[13] Szegedy C., Wei Liu, Chapel Hill, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, Andrew Rabinovich Going Deeper with Convolutions. 2014. – URL: https://arxiv.org/pdf/1409.4842 (дата обращения: 12.01.2026)

[14] Simonyan K., Zisserman A. Very Deep Convolutional Networks for Large-Scale Image Recognition. 2015. Published as a conference paper at ICLR 2015. – URL: https://arxiv.org/pdf/1409.1556 (дата обращения: 10.01.2026).

[15] Wei Liu, Anguelov D., Erhan D., Szegedy C., Reed S., Cheng-Yang Fu, Berg A.C. SSD: Single Shot MultiBox Detector. 2016. – URL: https://arxiv.org/pdf/1512.02325 (дата обращения: 11.01.2026).

[16] Официальный сайт ONNX. – URL: https://onnx.ai/.

[17] Основы технологий искусственного интеллекта: учебное пособие/ А.А. Семенов, В.В. Гончар, А.С. Эрдниев. – Московский университет МВД России имени В.Я, Кикотя, 2025. – 190с.

[18] Финансовый мониторинг: учебное пособие / В.И. Глотов, А.У. Альбеков, О.Н. Тисен и др. – КноРус, 2022. – 198 с.

[19] Тисен О.Н. Противодействие современным приемам и способам вербовки в международные террористические организации // Российская юстиция. 2018, №9. С. 51-54.

[20] Гончар В.В. О важности формирования единообразного понятийного аппарата необходимого для расследования преступлений в сфере компьютерной информации// Вестник Экономической безопасности. 2018. №1. С. 225-230.

[21] Орлова А.А., Гончар В.В. Особенности расследования преступлений, совершаемых в сфере информационных технологий // Безопасность бизнеса. 2021. № 4. С. 25-29.

References:

[1] Chen Zhang, Joohee Kim Video object detection with two-path convolutional LSTM pyramid. 2016. – URL: https://www.researchgate.net/publication /343702579_Video_Object_Detection_With_ Two-Path_ Convolutional_LSTM_ Pyramid/fulltext/5f3b2658928 51cd302013482/Video-Object-Detection-With-Two-Path-Convolutional-LSTM-Pyramid.pdf/ (дата обращения: 16.01.2026).

[2] Hanson A., Koutilya PNVR, Sanjukta Krishnagopal, Larry Davis Bidirectional Convolutional LSTM for the Detection of Violence in Videos. 2018. – URL: https://openaccess.thecvf.com/content_eccv_2018_workshops/w10 /html/Hanson_Bidirectional_Convolutional_LSTM_or_the_ Detection_of_Violence_in_ Videos_ ECCVW_2018_paper.html (дата обращения: 15.01.2026).

[3] Howard A.G., Menglong Zhu, Bo Chen, Kalenichenko D. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. 2017. - URL: https://arxiv.org/pdf/1704.04861/ (access date: 11.01.2026).

[4] Iandola F.N., Han S., Moskewicz M.W., Ashraf K., Dally W.J.,Keutzer K. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size Recognition. 2016. Published as a conference paper at ICLR. 2015. – URL: https://www. researchgate.net/publication/ 301878495_SqueezeNet_AlexNet-level_accuracy_ with_50x_fewer_ parameters_ and_05MB_model_size (дата обращения: 10.01.2026).

[5] Ioffe S., Szegedy C. Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. 2015. –URL: https://arxiv.org/pdf/1502.03167/ (access date: 13.01.2026).

[6] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun Deep Residual Learning for Image Recognition. 2015. – URL: https://arxiv.org/pdf/1512.03385 (access date: 11.01.2026).

[7] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun Spatial pyramid pooling in deep convolutional networks for visual recognition. 2015. - URL: https://arxiv.org/pdf/1406.4729/ (access date: 11.01.2026).

[8] Krizhevsky I., Sutskever I., Hinton G.E. Imagenet classification with deep convolutional neural networks. 2012. - URL: https://proceedings.neurips.cc/paper_files/paper/2012/file/c399862d3b9d-6b76c8436e 924a68c45b-Paper.pdf (accessed on: 12.01.2026).

[9] Lavin A., Scott Gray Fast Algorithms for Convolutional Neural Networks. 2015. - URL: https://arxiv.org/abs/1509.09308 (access date: 11.01.2026).

[10] Mikolov T., Kai Chen, Corrado G., Jeffrey Dean Efficient Estimation of Word Representations in Vector Space. 2013. – URL: https://arxiv.org/abs/1301.3781 (access date: 15.01.2026).

[11] Norman P. Jouppi, Cliff Young, Nishant Patil and others In-Datacenter Performance Analysis of a Tensor Processing Unit. 2017. – URL: https://arxiv.org/pdf/1704.04760 (access date: 11.01.2026).

[12] Ronneberger O., Fischer Ph., Brox Th. U-Net: Convolutional Networks for Biomedical Image Segmentation. 2015. – URL: https://arxiv.org/pdf/1505.04597/ (access date: 13.01.2026).

[13] Szegedy C., Wei Liu, Chapel Hill, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, Andrew Rabinovich Going Deeper with Convolutions. 2014. – URL: https://arxiv.org/pdf/1409.4842 (accessed on: 12.01.2026)

[14] Simonyan K., Zisserman A. Very Deep Convolutional Networks for Large-Scale Image Recognition. 2015. Published as a conference paper at ICLR 2015. - URL: https://arxiv.org/pdf/1409.1556 (access date: 10.01.2026).

[15] Wei Liu, Anguelov D., Erhan D., Szegedy C., Reed S., Cheng-Yang Fu, Berg A.C. SSD: Single Shot MultiBox Detector. 2016. – URL: https://arxiv.org/pdf/1512.02325 (access date: 11.01.2026).

[16] ONNX official website. – URL: https://onnx.ai/.

[17] Fundamentals of artificial intelligence technologies: a textbook/A.A. Semenov, V.V. Gonchar, A.S. Erdniev. - Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya, Kikotya, 2025. - 190s.

[18] Financial monitoring: training manual/V.I. Glotov, A.U. Albekov, O.N. Tisen et al. - KnoRus, 2022. - 198 s.

[19] Tisen O.N. Countering modern methods and methods of recruitment to international terrorist organizations//Russian Justice. 2018, №9. S. 51-54.

[20] Gonchar V.V. On the importance of forming a uniform conceptual apparatus necessary for investigating crimes in the field of computer information// Bulletin of Economic Security. 2018. №1. S. 225-230.

[21] Orlova A.A., Gonchar V.V. Features of the investigation of crimes committed in the field of information technology//Business security. 2021. № 4. S. 25-29.