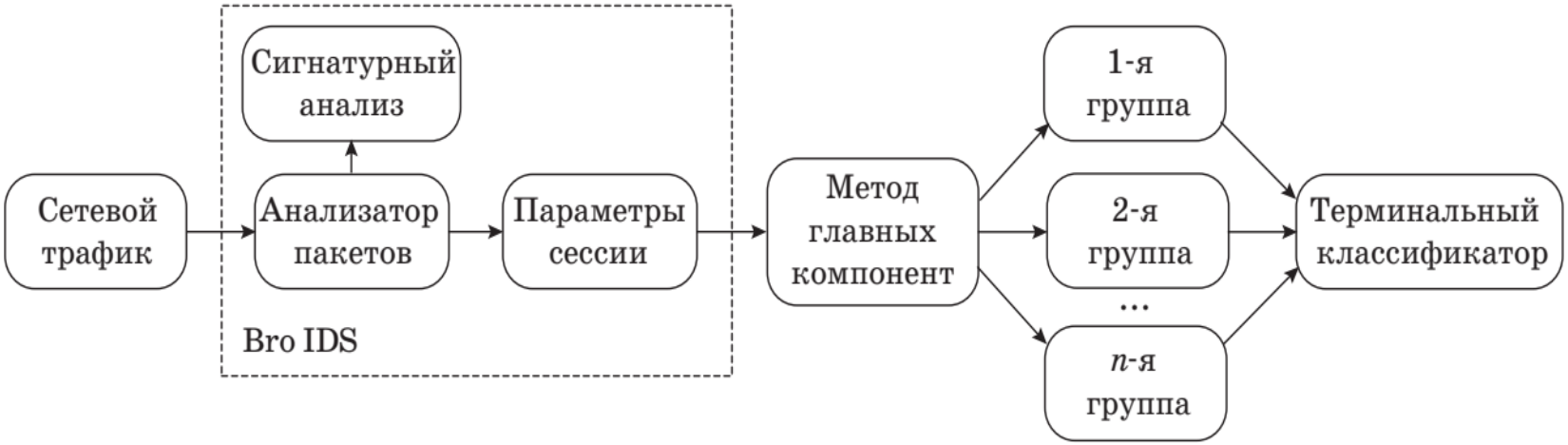
НЕЙРОСЕТЕВЫЕ КЛАССИФИКАТОРЫ В ЗАДАЧЕ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

Скобцов Вадим Юрьевич
Кандидат технических наук, доцент, доцент кафедры компьютерных технологий и программной инженерии,
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Касанин Сергей Николаевич,
Заместитель генерального директора, кандидат технических наук, доцент
Дмитриев Владимир Александрович,
Кандидат физ.-мат. наук, зав. лабораторией проблем защит информации
Объединенный институт проблем информатики Национальной академии наук Беларуси

Актуальность

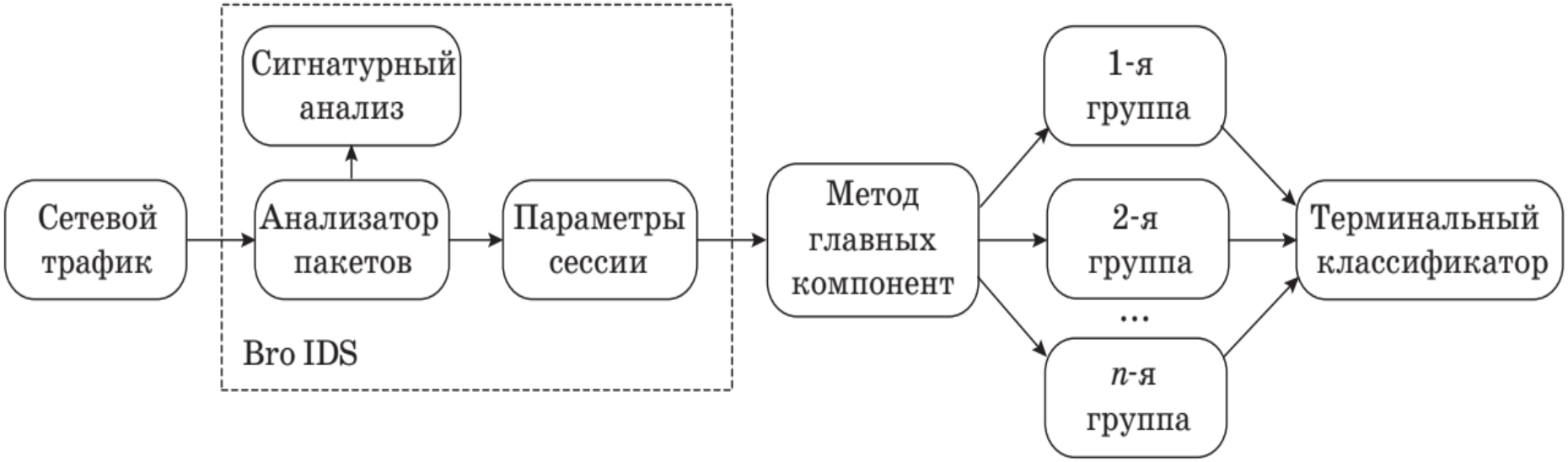
- В условиях появления принципиально новых классов сложных информационных систем (ИС) проблема оценивания их состояния выступает в качестве стратегического направления автоматизации и интеллектуализации соответствующих процессов в различных областях науки и техники.
- Высокая степень сложности современных ИС формируют высокие требования к точности, эффективности и универсальности методов контроля и диагностики нештатных ситуаций, что делает зачастую недостаточным использование только традиционных методов. Возможным дополнением является определение состояния информационной системы на основе интеллектуального анализа данных функционирования ИС, выявления нештатных ситуаций или аномального поведения.
- Одной из ключевых задач определения нештатных ситуаций в современных ИС является задача обнаружения вторжений (ОВ). Перспективным является интеграция поведенческих методов ОВ и методов ОВ на основе моделей машинного обучения на базе гибридного подходов.
- Методы машинного обучения в последнее десятилетие находят активное эффективное применение в различных практических задачах, в том числе анализа и обработки данных большого объема (Big Data), к которым можно отнести и данные анализируемого сетевого траффика ИС, где только за один день объем данных может составить сотни гигабайт информации.

Предполагаемая архитектура системы ОВ (СОВ)



- В предполагаемой СОВ на первом этапе осуществляется IP-дефрагментация сырых пакетов и сборка TCP-сегментов в сессии. Кроме того, этот этап отвечает за первоначальное обнаружение сетевых аномалий путем проверки соответствия содержимого отдельных пакетов заданным регулярным выражениям в сигнатурном множестве.
- Второй этап включает применение методов преобразования пространства данных выходных параметров сессий в сжатый набор атрибутов – компактное пространство информативных признаков меньшей размерности. Здесь возможно применение методов главных компонент или методов спектрального анализа данных.
- Третий этап представляет собой применение нескольких групп адаптивных классификаторов. Каждая группа состоит из детекторов, отвечающих за распознавание одного определенного типа соединения. Для повышения скорости классификации каждый детектор обрабатывает входящий набор параметров параллельно с остальными.

Предполагаемая архитектура системы ОВ (СОВ)



- Итоговый классификатор может быть представлен несколькими типами ансамблевых классификаторов: бэггинг, бустинг и тп.
- В качестве базового классификатора предлагается применять одну из наиболее широко используемых моделей машинного обучения на текущий день – нейронную сеть (НС).
- К преимуществам СОВ на основе искусственных НС можно отнести большую гибкость, параллелизм архитектуры нейронных сетей, особенно глубоких сетей, который позволяет одновременно эффективно иерархически анализировать признаки разных типов вторжений. Нейронная сеть будет быстро анализировать тип вторжений, которые являются регулярными, и выделять, изучать и распознавать инвариантные шаблоны таких вторжений. Это не только повышает точность, но и снижает возможность ложного срабатывания.

Описание данных трафика ИС

- Исходные данные трафика ИС являются временным рядом, который можно представить как матрицу $\boldsymbol{X} = (x_{ij})$, где *i*–я строка $\boldsymbol{X}_i$ является анализируемым вектором признаков трафика ИС в *i* – й момент времени, индекс *j* соответствует *j*–му показателю трафика ИС в *i*–м векторе $\boldsymbol{X}_i$.
- Данные трафика ИС являются *M*–мерным временным рядом $\boldsymbol{X} = (\boldsymbol{X}_1, \boldsymbol{X}_2, \dots, \boldsymbol{X}_M)$, каждый элемент которого $\boldsymbol{X}_j$ является столбцом матрицы данных трафика ИС $\boldsymbol{X}$ и в тоже время одномерным временным рядом, описывающим поведение *j*–го показателя трафика ИС на отрезке дискретных моментов времени $[1, T]$.

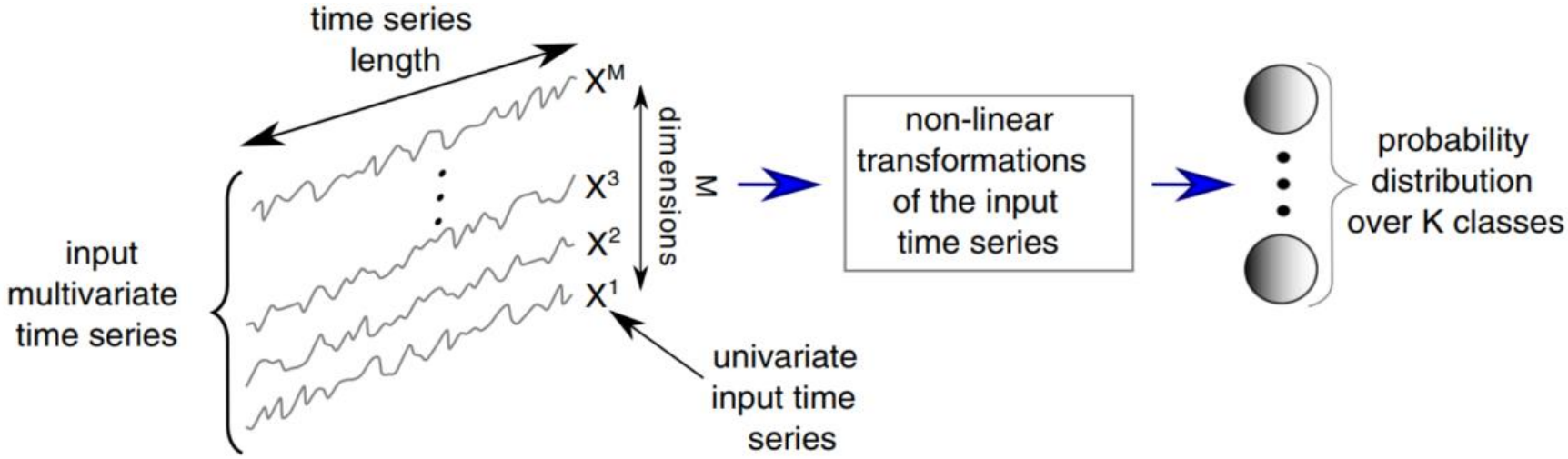
Проблема анализа данных трафика ИС

Domain	Context	Problem statement
Требуется проанализировать данные трафика ИС с целью определения наличия или отсутствия вторжения (нештатное или штатное состояния).	Последние исследования показали, что нейросетевые модели работают лучше для задачи анализа данных временных рядов.	1. Исследование и разработка гибридных алгоритмов анализа данных ТМИ на основе моделей нейронных сетей и машинного обучения. 2. Разработка и исследование автоматического метода поиска оптимальных гибридных нейросетевых моделей классификации данных временных рядов.

Почему «классические» модели машинного обучения непрактичны для больших данных

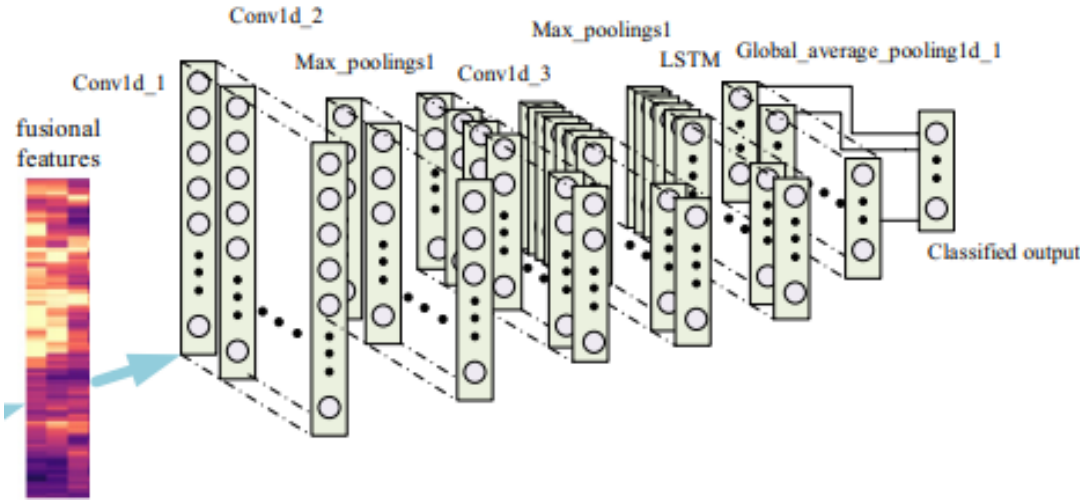
- Свежие публикации сосредоточены на разработке методов ансамбля. Эти подходы используют либо ансамбль деревьев решений (случайный лес), либо ансамбль различных типов дискриминантных классификаторов (машины опорных векторов (SVM), классификаторы k ближайших соседей (kNN) с несколькими функциями расстояния) на одном или нескольких пространствах признаков. Большинство из этих подходов имеют этап предобработки данных, на котором преобразуются исходные временные ряды.
- Этот подход стимулировал разработку ансамбля из 35 классификаторов COTE (Collective Of Transformation-based Ensembles), который не только объединяет разные классификаторы для одного и того же преобразования, но объединяет разные классификаторы для разных представлений разных временных рядов. Преимущества COTE были улучшены с помощью иерархической системы голосования, получив метод HIVE-COTE. HIVE-COTE в настоящее время считается одним из ведущих алгоритмов классификации временных рядов среди классических моделей машинного обучения при оценке 85 наборов данных из архива UCR/UEA. Для достижения высокой точности HIVE-COTE становится чрезвычайно требовательным в вычислительном отношении и часто непрактичным для решения реальных задач интеллектуального анализа больших данных.
- Этот подход требует обучения тридцати семи классификаторов, а также перекрестной проверки каждого гиперпараметра этих алгоритмов, что делает невозможным обучение этого подхода в некоторых ситуациях. Чтобы подчеркнуть эту невозможность, заметим, что одним из этих тридцати семи классификаторов является Shapelet преобразование, временная сложность которого равна $O(n^2 l^4)$, где n — количество одномерных временных рядов в наборе данных, а l — длина временного ряда.
- H. Ismail Fawaz, G. Forestier, J. Weber, L. Idoumghar, P. Muller “Deep learning for time series classification: a review”. Data Mining and Knowledge Discovery. 2019; 33: 917–963.

Проблема классификации данных трафика ИС на k классов – состояний

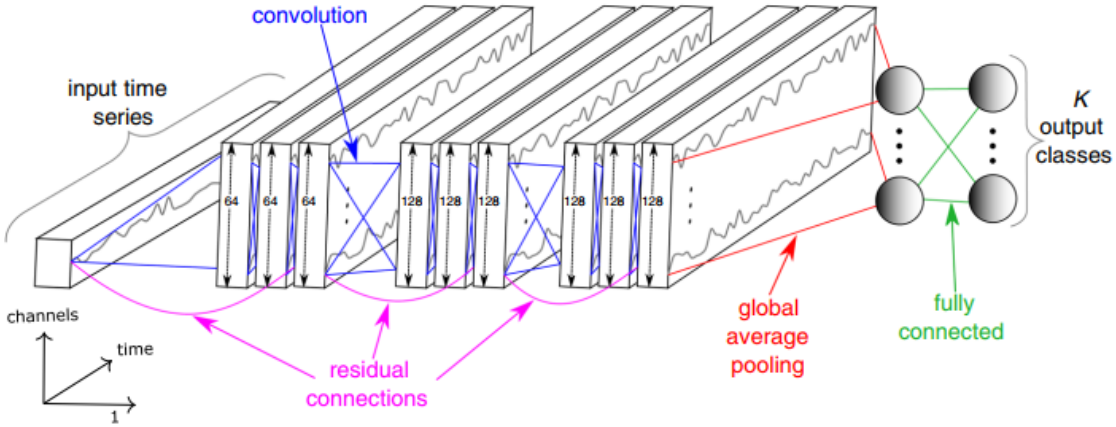


- При условии наличия эталонной целевой информации – меток состояний наличия или отсутствия вторжения в ИС – для данных трафика ИС для каждого вектора показателей в *i* –й момент времени $\boldsymbol{X}_i$ в соответствие поставлена метка класса $y_i \in \boldsymbol{Y}$,которая характеризует состояние ИС в контексте сетевого вторжения. Для автоматического определения состояния ИС решается задача k-классовой классификации, где k – общее число состояний, определяемое экспертом. Конечной целью является классификация векторов $\boldsymbol{X}_i$ M-мерного временного ряда $\boldsymbol{X}$ ТМИ к 1 штатному и k-1 нештатным состояниям. Мы решаем задачу для k=2 – наличие или отсутствие вторжения в ИС.

Гибридные глубокие нейросетевые классификаторы



- Отличие ResNet архитектур от обычных сверточных сетей заключается в добавлении линейных связей, чтобы связать выход более раннего остаточного блока слоев с входами более позднего блока, что позволяет потоку градиента распространяться напрямую через эти соединения. Это значительно упрощает обучение сети за счет уменьшение эффекта исчезающего градиента.



- Chen, Haoze. Hybrid neural network based on novel audio feature for vehicle type identification / Haoze Chen, Zhijie Zhang // 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC): proceedings of the international conference (25–28 May 2020). – 2021.
- Zhao N. Combination of Convolution-al Neural Network and Gated Recurrent Unit for Aspect-Based Sentiment Analysis / N. Zhao // IEEE Access. – Vol. 9. – 2021. – P. 15561-15569.
- Kaiming, He., et al. “Deep Residual Learning for Image Recognition”. Conference on Computer Vision and Pattern Recognition. 2015. – Available at: https://arxiv.org/abs/1512.03385

Архитектура разработанных гибридных нейросетвых классификационных моделей

Z_1 = Conv1D(filters=n, kernel_size=k1, activation='AF1') (X_i)
Z_1 = Conv1D(filters=n, kernel_size=k1, activation=' AF1') (Z_1) * C1 слоев
Z_2 = add([Z_1, X_i]) – остаточная связь of X_i
Z_2 = AveragePooling1D(p)(Z_2)
Z_3 = Conv1D(filters=n, kernel_size=k2, activation=' AF1') (Z_2)
Z_3 = Conv1D(filters=n, kernel_size=k2, activation=' AF1') (Z_2) * C2 слоев
Z_4 = AveragePooling1D(p)(X_i)
Output = add([Z_2, Z_3, Z_4]) – остаточная связь of Z_2 and Z_3
Output = GRU(units=r)
Output = Dense(d, activation=' AF1') (Output) * C3 слоев
Output = Dense(k, activation=' AF2') (Output)

Изначально на основе предложенной архитектуры были получены гибридные нейросетевые классификаторы, решающие задачу определения штатного и нештатных категориальных состояний на основе анализа данных временных рядов телеметрической информации (ТМИ) бортовой аппаратуры группировки малых КА АИСТ Самарского национального исследовательского университета имени академика С.П.Королёва. Рассматривалась трех-классовая задача классификации для определения штатного и нештатного состояний космических аппаратов.

1. В.Ю.Скобцов, Б.В.Соколов Гибридные нейросетевые модели в задаче мультиклассовой классификации данных телеметрической информации малых космических аппаратов // Вестник ВГУ. Системный анализ и информационные технологии, 2022, № 3, С.99-114.
2. Скобцов В. Ю., Соколов Б. В., Чжан В.-А., Фу М. Гибридные нейросетевые модели мониторинга данных временных рядов сложных объектов // Изв. вузов. Приборостроение. 2024. Т. 67, № 2. С. 200—204.

Сравнительный анализ нейросетевых моделей для задачи классификации данных ТМИ АИСТ

- Для задачи многоклассовой классификации на данных ТМИ МКА АИСТ для разработанной гибридной нейросетевой модели с использованием остаточных связей по технологии ResNet были получены точности: ~0.998 (этап обучения), ~0.981 (этап валидации) и ~0.985 (этап тестирования). Выполнен сравнительный анализ полученной гибридной нейросетевой модели с набором распространенных глубоких нейросетевых классификаторов, показавший преимущество полученного решения по точности классификации на этапе тестирования для всех сравниваемых моделей на 1–7%, по времени обучения и валидации почти для всех сравниваемых моделей получено преимущество в 1.5–4 раза.

Тип нейросетевой модели	Обучающий набор		Валидационный набор		Тестовый набор		Время обучения одной эпохи, сек
	Точность	Функция потерь	Точность	Функция потерь	Точность	Функция потерь	
LeNet	0.9977	0.0111	0.9744	0.2584	0.9757	0.1947	1
AlexNet	0.9988	0.0012	0.9697	0.3616	0.9682	0.2932	2
Xception	0.9988	0.0024	0.9744	0.1961	0.9646	0.2506	8
Yolo	0.9977	0.0127	0.9650	0.1918	0.9646	0.2602	1
MobileNet	0.9942	0.0221	0.9464	0.2811	0.9160	0.3289	3
Inception	0.9837	0.0607	0.9674	0.0927	0.9539	0.1154	4
ResNet	0.9942	0.0397	0.9782	0.0881	0.9757	0.0755	8
Hybrid_NN_TD_AIST	0.9977	0.0349	0.9814	0.0869	0.9851	0.0790	2

Гибридный нейросетевой классификатор обнаружения вторжений в ИС, разработанный вручную

- Исходя из эффективности разработанного гибридного нейросетевого классификатора, он был применен нами для решения задачи обнаружения сетевых вторжений на основе анализа данных сетевого трафика набора данных KDDCup 1999 Data . Для анализа было взято подмножество данного датасета размерностью 10000 векторов и преобразовано для решения задачи 2-классовой классификации с целью обнаружения сетевого вторжения в ИС (различные метки вторжений разных типов были помечены как 0 – класс состояния вторжения в ИС, 1 – класс штатного состояния ИС).
- В результате обучения, валидации и тестирования предложенной нами гибридной нейросетевой модели была получена точность классификации на этапе тестирования, равная 0.9994, что существенно превышает точность результата для ТМИ МКА АИСТ. Сложность гибридной НС в данном случае составляет 7714 синаптических коэффициентов и 25 нейронных слоев.

KDD Cup 1999 Data https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

Гибридные нейросетевой классификатор обнаружения вторжений в ИС, полученные автоматически с помощью AutoML генетического алгоритма

- С целью сокращения времени создания нейросетевых моделей был разработан генетический алгоритм автоматического поиска (AutoML) гибридных нейросетвых моделей, который был применен для решения задачи обнаружения сетевых вторжений в модифицированном наборе данных KDDCup.

Skobtsov, V.Y., Stasiuk, A. (2023). Automatic Searching the Neural Network Models for Time Series Classification of Small Spacecraft's Telemetry Data with Genetic Algorithms. In: Silhavy, R., Silhavy, P. (eds) Artificial Intelligence Application in Networks and Systems. CSOC 2023. Lecture Notes in Networks and Systems, Vol. 724., pp. 800–811.

- Предложенный autoML метод выполняет поиск не только значений гиперпараметров, но и полностью модели гибридной НС в целом заданной выше архитектуры.
- В результате работы генетического autoML метода в конце поиска были построены НС классификаторы с разными хромосомами − гибридными нейронными сетями, которые показали результаты, близкие к максимальному значению фитнесс функции − точности классификации, равной 1.0. Данный факт можно рассматривать как экспериментальное подтверждение построения решения, близкого к оптимальному, для определенных параметров поиска.

Гибридные нейросетевой классификатор обнаружения вторжений в ИС, полученные автоматически с помощью AutoML генетического алгоритма

- Поиск выполнялся на компьютере i5, ОЗУ 16Gb, GPU Nvidia GeForce RTX 3060 6Gb под управлением ОС Windows 10, на данных сетевого трафика KDDCup размерностью 10000 векторов за 9130 сек. Наилучшее значение фитнеса, достигнутое в ходе эксперимента, составляет 100%. В конце поиска (для популяции последнего поколения) было также замечено, что представители с разными хромосомами – нейронными сетями показали результаты, близкие к максимальному значению фитнесс функции.

fitness: 0.9994999766349792, *'num_params': 8930*

		conv_kernel_size	conv_n_filters	gru_n_units	dense_n_units
Conv1D	1	2	26	14	452
Conv1D	1	2	26	14	452
Conv1D	1	2	6	24	740
GRU	1	2	8	12	226
Flatten	1	2	28	10	358
Dense	1	2	6	10	398

fitness": 1.0, "num_params": 96686

		conv_kernel_size	conv_n_filters	gru_n_units	dense_n_units
Conv1D	1	2	40	12	442
Conv1D	1	2	26	14	452
GRU	1	2	8	12	226
Flatten	1	2	6	14	448
Dense	1	2	76	20	146
Dense	1	2	76	10	608

Заключение

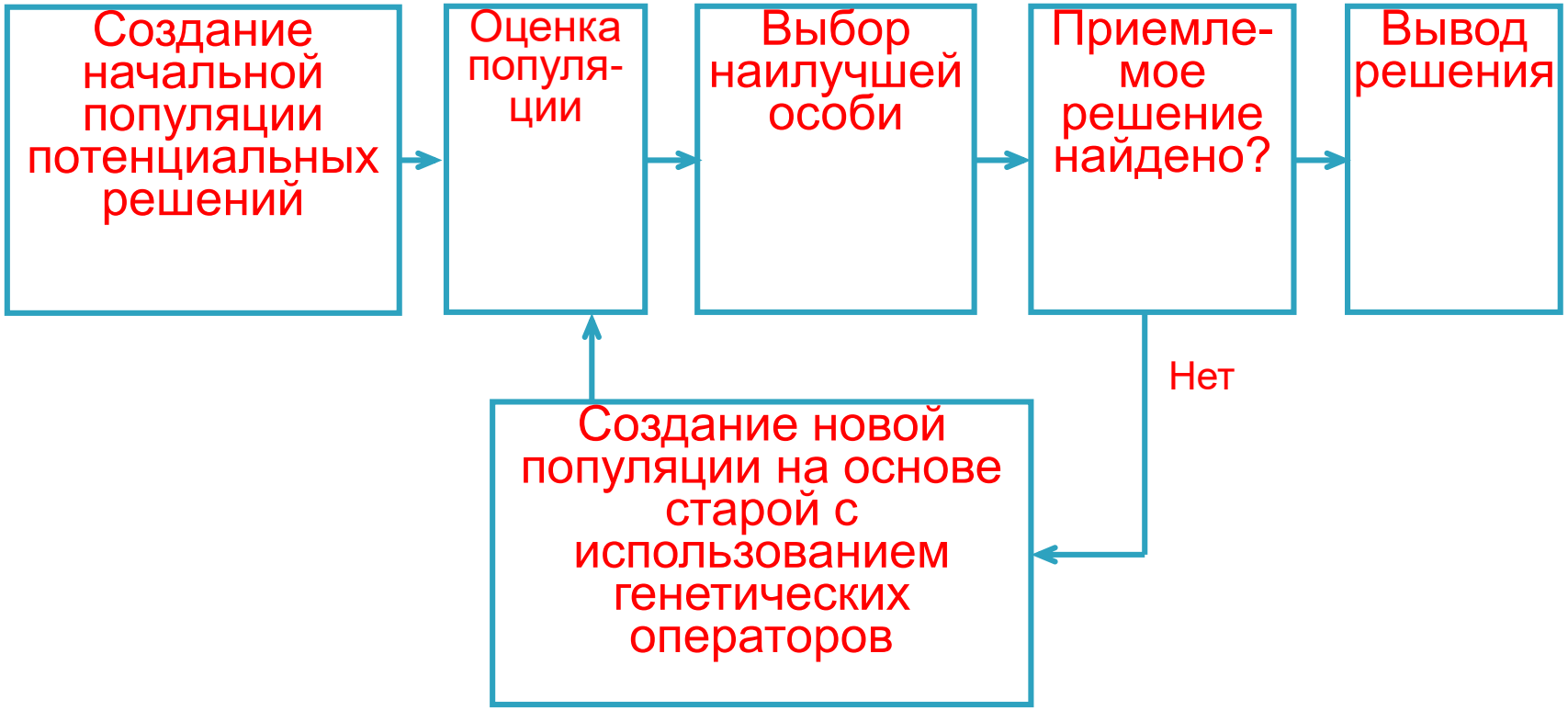
- В силу показанного выше преимущества гибридных нейросетевых моделей для решения задач анализа и мониторинга данных функционирования сложных объектов различной природы, в частности данных сетевого трафика ИС с целью обнаружения сетевых вторжений в ИС, перспективным является дальнейшее исследование гибридных нейросетевых моделей на основе их комплексирования с классическими моделями нелинейных отображений и фильтров, а также классическими моделями машинного обучения.

СПАСИБО ЗА ВНИМАНИЕ

E-mail: vasko_vasko@mail.ru

Генетический алгоритм автоматического поиска классификационных моделей анализ данных временных рядов на основе гибридных глубоких нейронных сетей

Генетический алгоритм



Структура хромосомы

Main genes in chromosome	
Gene	Possible values and restrictions
learning_rate	1e-1, 1e-2, 1e-3, 1e-4, 1e-5, 1e-6, 1e-7
optimizer	Adam, SGD, Adagrad
loss_function	categorical_crossentropy, poisson, kl_divergence
architecture	-
Functiomal genes in chromosome	
Gene	Comment
fitness	Collect fitness function value
num_params	Collect number of parameteres of neural network

Структура хромосомы архитектуры гибридной нейронной сети

Layer	on	Conv kernel size	Conv filters	GRU units	Dense units
Conv1D	1	2	16	10	584
Conv1D	1	4	32	22	236
Conv1D	1	2	112	20	364
GRU	1	10	8	24	526
Flatten	1	10	14	16	658
Dense	1	12	126	10	56
Dense	1	6	46	22	148

Фитнесс функция

- В контексте нейронных сетей точность прогнозирования выходных данных с учетом входных данных может использоваться в качестве фитнесс функции. Цель в этом случае — максимизировать точность сети на проверочном или тестовом наборе.
- Таким образом, фитнесс функция будет измерять, насколько хорошо сеть работает с набором данных, и назначать более высокие оценки приспособленности особям – нейронным сетям, которые дают лучшие результаты. Это можно использовать для оптимизации различных аспектов нейронной сети, таких как архитектура, гиперпараметры или веса сети.

Оператор кроссинговера

Gene	Parent 1	Offspring	Parent 2
learning_rate	1e-3	1e-3	1e-6
loss	poisson	kl_divergence	kl_divergence
optimizer	Adam	SGD	SGD
architicture	–custom–	–custom–	–custom–

	Layer	on	CS^1	CF^2	GU^3	DU^4
Parent 1	Conv1D	1	2	16	10	584
	GRU	1	10	8	24	526
	Flatten	1	10	14	16	658
	Dense	1	12	126	10	56
Parent 2	Conv1D	1	4	8	18	268
	Flatten	1	6	32	4	102
	Dense	1	8	26	10	344
	Dense	1	2	6	2	38
	Dense	1	2	12	20	186

*

	on
Random binary mask	1
	1
	0
	1
	0
	1
	0
	0
	1

=

	Layer	on	CS^1	CF^2	GU^3	DU^4
Offspring	Conv1D	1	2	16	10	584
	GRU	1	10	8	24	526
	Dense	1	12	126	10	56
	Flatten	1	6	32	4	102
	Dense	1	2	12	20	186

CS^1 - Conv kernel size; CF^2 - Conv filters; GU^3 - GRU units; DU^4 - Dense units;

Оператор мутации

- Мы используем случайное переопределение значение гена в качестве оператора мутации. Мутация одного из генов выполняется с вероятностью 15%. Значения генов Learning_rate, loss_fuction и оптимизатора определяются из набора возможных значений для этого гена. Мутация гена nn_architecture представляет собой совершенно новую архитектуру, созданную случайным образом.

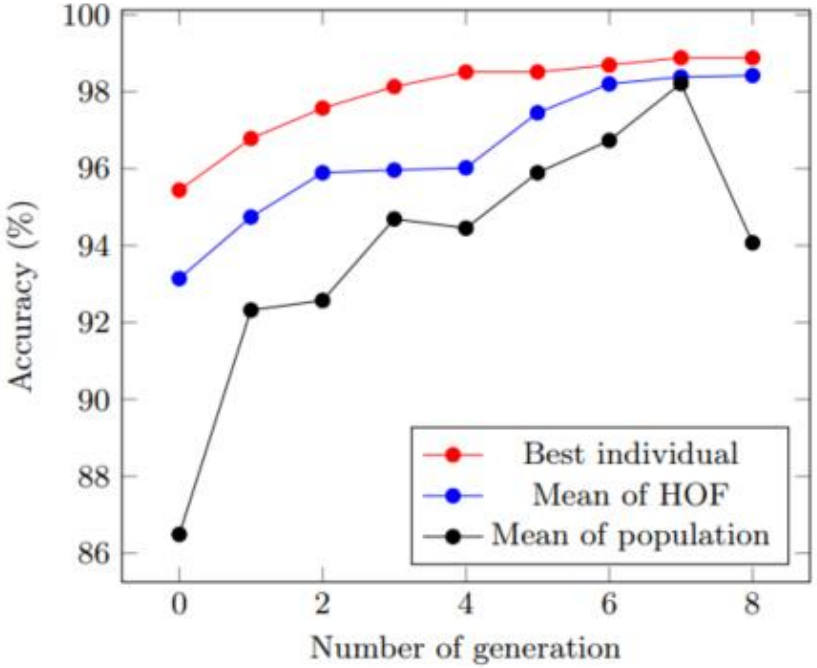
Оператор селекции

- В качестве механизма селекции была выбрана методика **Зала славы** (Hall of fame -HOF).
- HOF— это метод, используемый в генетических алгоритмах для улучшения процесса селекции. В типичном генетическом алгоритме отбор осуществляется на основе значений фитнесс функций, при этом особи с более высокими значениями с большей вероятностью будут выбраны для воспроизводства.
- Однако метод HOF отслеживает лучших особей, встреченных в процессе эволюции, и сохраняет их в отдельном списке. Эти особи не подвергаются «давлению» со стороны оператора селекции, и их разрешено оставлять в популяции, даже если их фитнесс ниже, чем у других особей.

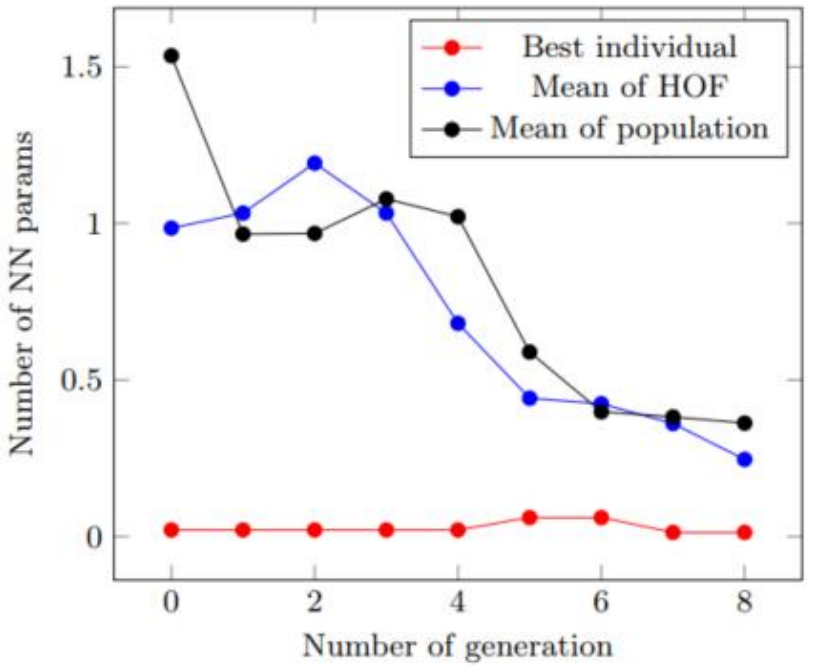
```
63/63 [==============================] - 1s 5ms/step - loss: 4.0428e-05 - accuracy: 1.0000
63/63 [==============================] - 1s 5ms/step - loss: 0.5031 - accuracy: 0.9995
63/63 [==============================] - 1s 5ms/step - loss: 0.0036 - accuracy: 0.9995
63/63 [==============================] - 1s 5ms/step - loss: 0.0093 - accuracy: 0.9990
63/63 [==============================] - 1s 5ms/step - loss: 0.0080 - accuracy: 0.9995
63/63 [==============================] - 1s 6ms/step - loss: 0.0035 - accuracy: 0.9995
63/63 [==============================] - 1s 5ms/step - loss: 0.1286 - accuracy: 0.9810
63/63 [==============================] - 1s 6ms/step - loss: 0.0054 - accuracy: 0.9990
[[0.9994999766349792, 103056], [0.9994999766349792, 16852], [0.9994999766349792, 213074], [0.9994999766349792, 6386], [0.999499
9766349792, 94314], [0.9994999766349792, 32842], [1.0, 593582], [1.0, 96686]]
--- 9129.489754199982 seconds ---
```

Результаты для ТМИ МКА АИСТ

- Наилучшее значение фитнеса, достигнутое в ходе эксперимента, составляет 98,8%. В конце поиска (для популяции последнего поколения) было замечено, что представители с разными хромосомами – нейронными сетями показали результаты, близкие к максимальному значению фитнесс функции. Данный факт можно рассматривать как экспериментальное подтверждение найденного решения, близкого к оптимальному для определенных параметров поиска.



(a) Fitness of individuals



(b) Number of neural network params

Fig. 4: Genetic algoritm work process artifacts

Примеры построенных гибридных НС

	type	on	conv_kernel_size	conv_n_filters	gru_n_units	dense_n_units		
0	Conv1D	1	2	16	10	584		
1	Conv1D	1	2	16	10	584		
3	GRU	1	10	8	24	526		
5	Flatten	1	10	14	16	658		
7	Dense	1	2	60	24	516		
9	Dense	1	8	18	8	352		
10	Dense	1	2	60	24	516	0.9888059496879578	382439

, [0.9813432693481445, 21171]]

	type	on	conv_kernel_size	conv_n_filters	gru_n_units	dense_n_units		
1	Conv1D	1	2	16	10	584		
2	Conv1D	1	2	32	22	236		
3	Conv1D	1	2	112	20	364		
4	GRU	1	10	8	24	526		
5	Flatten	1	10	14	16	658		
6	Dense	1	12	126	10	56	0.9813432693481445	21171

	type	on	conv_kernel_size	conv_n_filters	gru_n_units	dense_n_units		
0	Conv1D	1	4	66	24	76		
1	Flatten	1	8	108	12	226		
2	Dense	1	2	60	24	516	0.9813432693481445	786213

Результаты для ТМИ ЗД БКА

- Поиск выполнялся на компьютере i5, ОЗУ 16Gb, GPU Nvidia GeForce RTX 3060 6Gb под управлением ОС Windows 10, на подмножестве исходных данных ТМИ ЗД БКА размерностью 5000 векторов в силу большой временной сложности 11757 сек. Наилучшее значение фитнеса, достигнутое в ходе эксперимента, составляет 98%. В конце поиска (для популяции последнего поколения) было также замечено, что представители с разными хромосомами – нейронными сетями показали результаты, близкие к максимальному значению фитнесс функции.

'fitness': 0.9789999723434448, 'num_params': 500644

Conv1D	1	2	28	12	244
GRU	1	2	28	18	964
Flatten	1	2	34	26	730
Dense	1	2	76	10	608
Dense	1	2	6	10	398
Dense	1	2	76	10	608

'fitness': 0.9800000190734863, 'num_params': 582524

Conv1D	1	2	28	12	244
GRU	1	2	28	18	964
Flatten	1	2	34	26	730
Dense	1	2	76	10	608
Dense	1	2	6	10	398
Dense	1	2	76	10	608
Dense	1	2	102	28	136

Преимущество и новизна

1. Разработанное методическое и программное обеспечение методики и программного модуля интеллектуального анализа данных ТМИ МКА/СлТО с одной стороны обеспечивают автоматизированную поддержку принятия решения экспертом НКУ о техническом состоянии МКА и его компонентов путем выделения состояний функционирования МКА на основе методов кластерно-классификационного анализа данных ТМИ и расчетной оценки среднего числа нештатных ситуаций при условии отсутствия в обучающей выборке информации об эталонной разметке состояний.

2. При условии наличия такой эталонной информации методы классификации данных ТМИ МКА на основе глубоких гибридных нейросетевых моделей позволяют определять техническое состояние МКА и его подсистем автоматически.

Преимущество и новизна

3. Предложенный генетический алгоритм автоматического поиска гибридных нейросетевых моделей классификации позволяет:

- существенно сократить время поиска, систематизировать и автоматизировать процесс построения по сравнению с ручной разработкой нейросетевых моделей для задачи классификации данных телеметрии;
- улучшить результаты для ранее построенных гибридных нейронных моделей с одной стороны, с другой стороны – построить более простые модели с высокой точностью классификации, сравнимой с достигнутой;
- стабильно воспроизводить достаточно высокую точность классификации для разных моделей.

4. Полученные ГА результаты можно рассматривать как подтверждение нахождения близкого к оптимальному решения для определенных параметров эксперимента.

Преимущество и новизна

5. Разработанная методика и программный модуль прошли апробацию на данных реальной ТМИ с МКА двух типов: ЗД Белорусского космического аппарата и МКА АИСТ Самарского национального исследовательского университета имени академика С.П.Королева, также на данных ТМИ сетевого трафика датасета Kddcup. Апробация показала:

- их эффективность для данных различной размерности;
- высокую точность разработанной методики и программных средств и их преимущество по сравнению с известными моделями машинного обучения как по точности классификационно-кластерного анализа, так и по сокращению времени обучения.

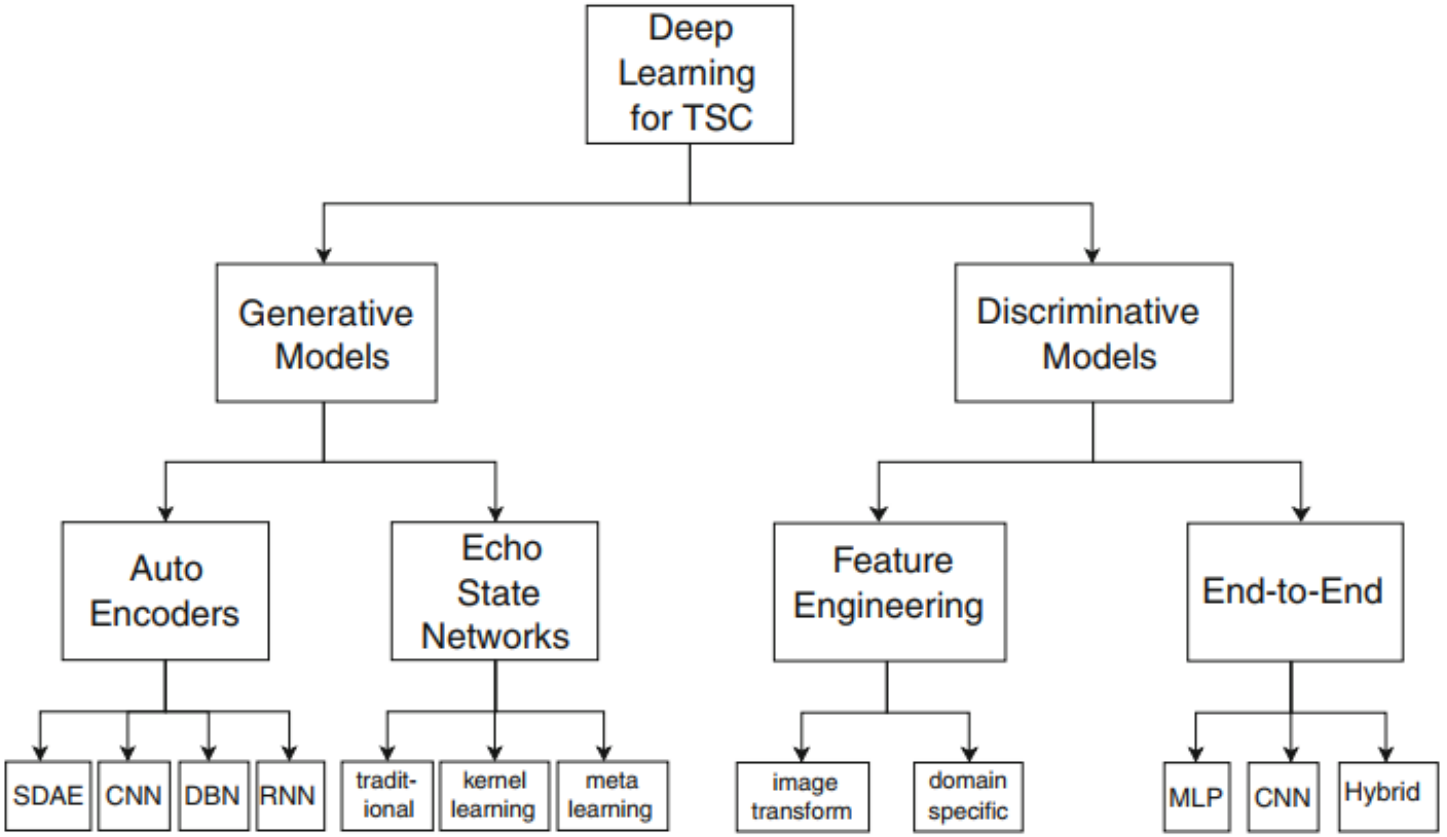
6. Для задачи бинарной классификации на данных ТМИ БКА разработанная гибридная нейросетевая модель с использованием остаточных связей сравнима по точности с нейросетевой классификационной моделью Inception (остальные классификаторы имеют меньшую точность): ~0.98 (этап обучения), ~0.97 (этапы валидации и тестирования). При этом полученная гибридная модель в 2.5 раза быстрее по времени обучения и валидации и имеет более облегченную структуру, что важно для ее реализации.

Преимущество и новизна

6. Для данных ТМИ МКА АИСТ предложенная гибридная модель *Hybrid_NN_TD_AIST* превосходит известные глубокие нейросетевые модели. По времени одной эпохи обучения и валидации разработанная модель сравнима (2 сек.) с моделью AlexNet, но превосходит ее по точности классификации на этапе тестирования на 2 %. Модели LeNet и Yolo превосходят разработанную модель по времени — 1 сек. < 2 сек., но уступают по точности на этапе тестирования на 1-2 %. Остальные модели уступают предложенной модели по точности классификации на 1-7 % и по времени одной эпохи обучения и валидации в 1.5-4раза.

7. Сгенерированные автоматически с помощью разработанного ГА гибридные нейросетевые классификаторы по точности находятся на уровне или немного превосходят НС модели, разработанные вручную.

Different deep learning approaches for time series classification



- [1] H. Ismail Fawaz, G. Forestier, J. Weber, L. Idoumghar, P. Muller “Deep learning for time series classification: a review”. Data Mining and Knowledge Discovery. 2019; 33: 917–963. DOI: https://doi.org/10.1007/s10618-019-00619-1.

Reasons to investigate dicriminative end-to-end deep learning approaches for time series classification

- The main characteristic of a generative model is fitting a time series self-predictor whose latent representation is later fed into an off-the-shelf classifier such as Random Forest or SVM. Although these models do sometimes capture the trend of a time series, we decided to leave these generative approaches out of our experimental evaluation for the following reasons:
  - This type of method is mainly proposed for tasks other than classification or as part of a larger classification scheme (Bagnall et al. 2017);
  - The informal consensus in the literature is that generative models are usually less accurate than direct discriminative models (Bagnall et al. 2017; Nguyen et al. 2017);
  - The implementation of these models is usually more complicated than for discriminative models since it introduces an additional step of fitting a time series generator — this has been considered a barrier with most approaches whose code was not publicly available such as Gong et al. (2018), Che et al. (2017b), Chouikhi et al. (2018), Wang et al. (2017a);
  - The accuracy of these models depends highly on the chosen off-the-shelf classifier which is sometimes not even a neural network classifier (Rajan and Thiagarajan 2018).

Эксперименты

ГА поиск запускался на данных на машине Linux с 30 виртуальными ядрами ЦП. За все время работы алгоритма процессор был загружен на 27%. Эксперимент длится 2778 секунд. Алгоритм работы на Apple MacBook M1 Max задействовал примерно 95% ресурсов ЦП и занял 3586 секунд.

Эксперимент имел следующие параметры: численность популяции - 25, размер зала славы - 15, количество поколений - 8.

Parameter	Min	Max
Number Conv layers	2	8
Number Conv filters	4	128
Conv kernel size	2	16
Number GRU layers	0	3
Number GRU units	8	32
Number Dense layers	2	10
Number Dense units	16	1024
Probability occurance Dropout(0.2)	0.25	0.25

Table 2: Neural network architicture restrictions

6 270

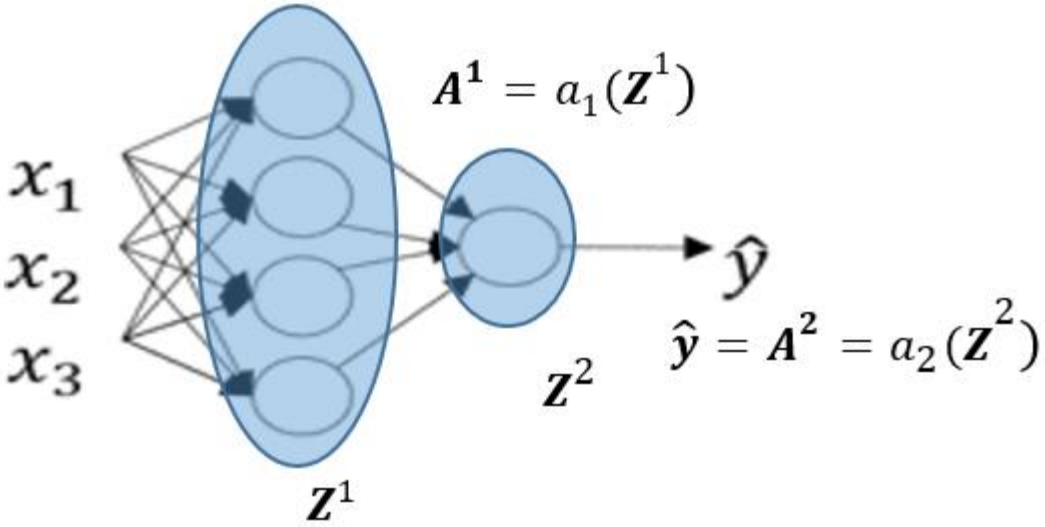
Полносвязные нейронные сети/слои

- Полносвязные нейронные сети/слои можно рассмотреть на примере следующей 2-слойной сети, которая представлена на рис.2 и задан формулами

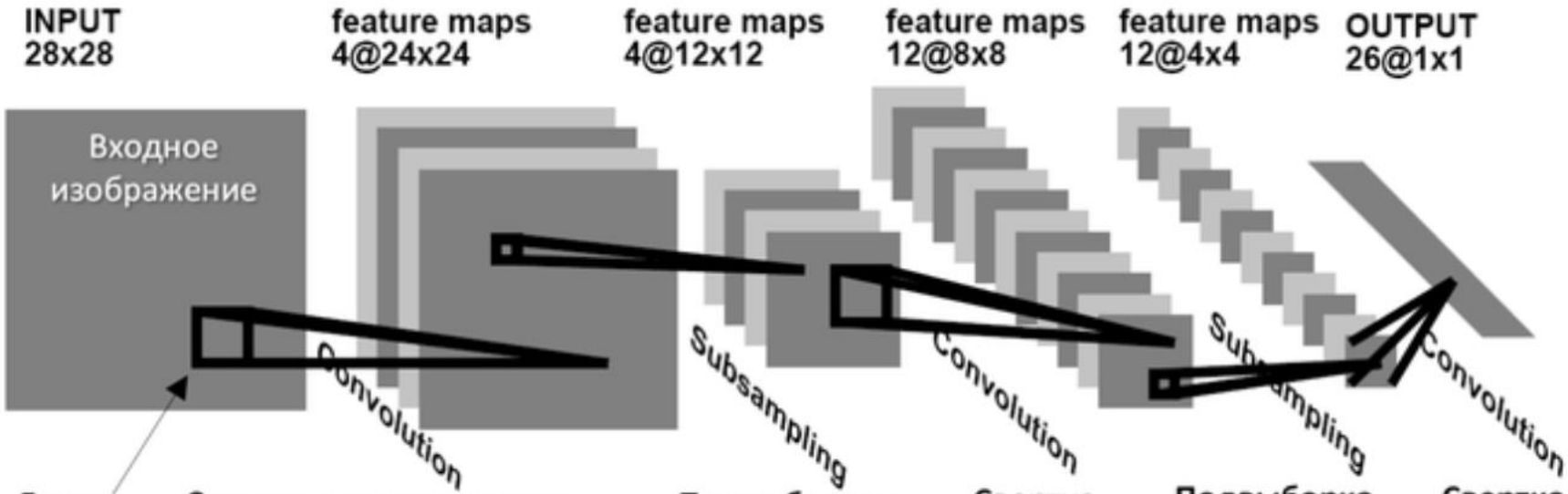
$\boldsymbol{Z^1 = W^1 X + b^1}$; $\boldsymbol{A^1 = a_1(Z^1)}$; $\boldsymbol{Z^2 = W^2 A^1 + b^2}$; $\boldsymbol{\hat{y} = A^2 = a_2(Z^2)}$,

где $\boldsymbol{W^i}$ – значения весовых коэффициентов,

$a_i(\boldsymbol{Z^i})$ – активационные функции слоев.



Сверточные нейронные сети/слои



Ядро свертки – матрица из весов, например, размером 5x5

Свертка – проход ядром свертки по всем нейронам нижнего слоя для активации нейронов верхнего слоя – получение карты признаков (feature maps). Для ядер разного типа получаются разные карты признаков.

Подвыборка – операция уменьшения размерности. Чаще всего – выбор максимума или поиск среднего по нескольким соседним нейронам.

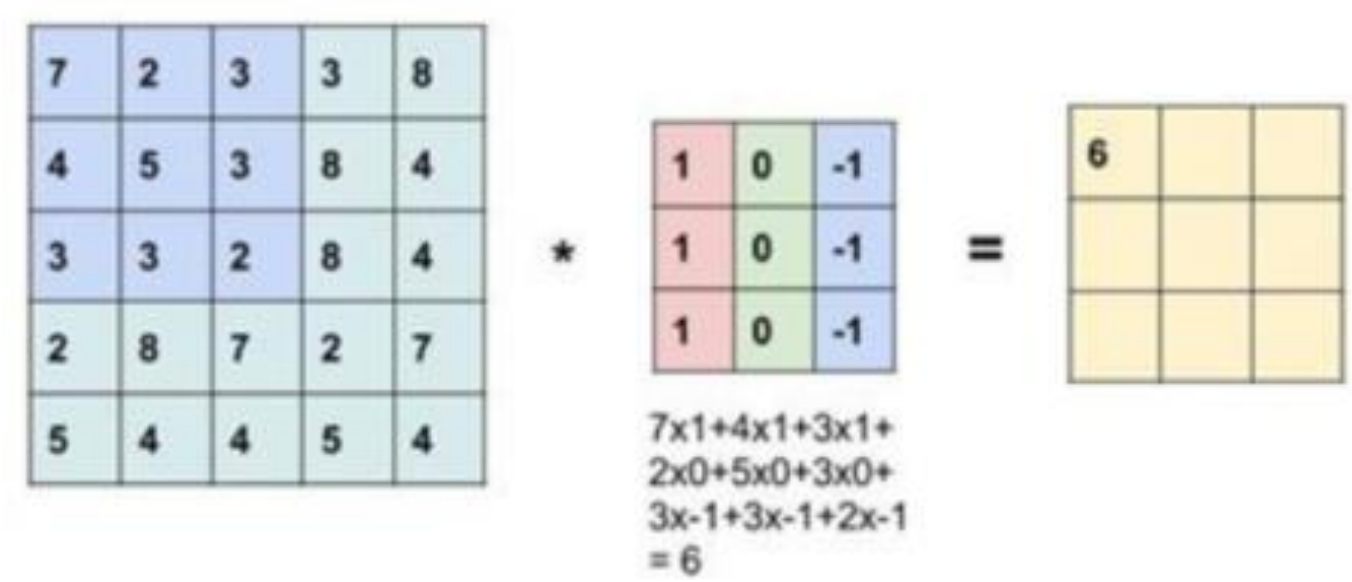
Свертка

Подвыборка

Свертка

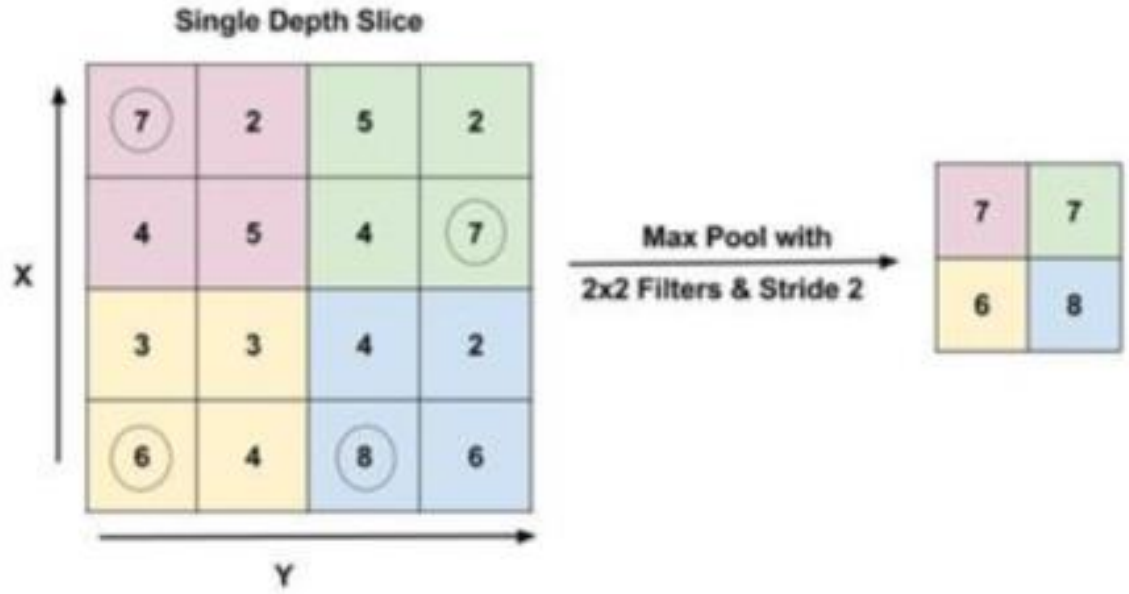
Сверточные нейронные сети/слои – операция свертки

- Свертку можно рассматривать как взвешенную сумму между двумя сигналами или функциями. Пример операции свертки на матрице размером 5 × 5 с ядром размером 3 × 3 показан ниже. Ядро свертки скользит по всей матрице для получения карты активации.



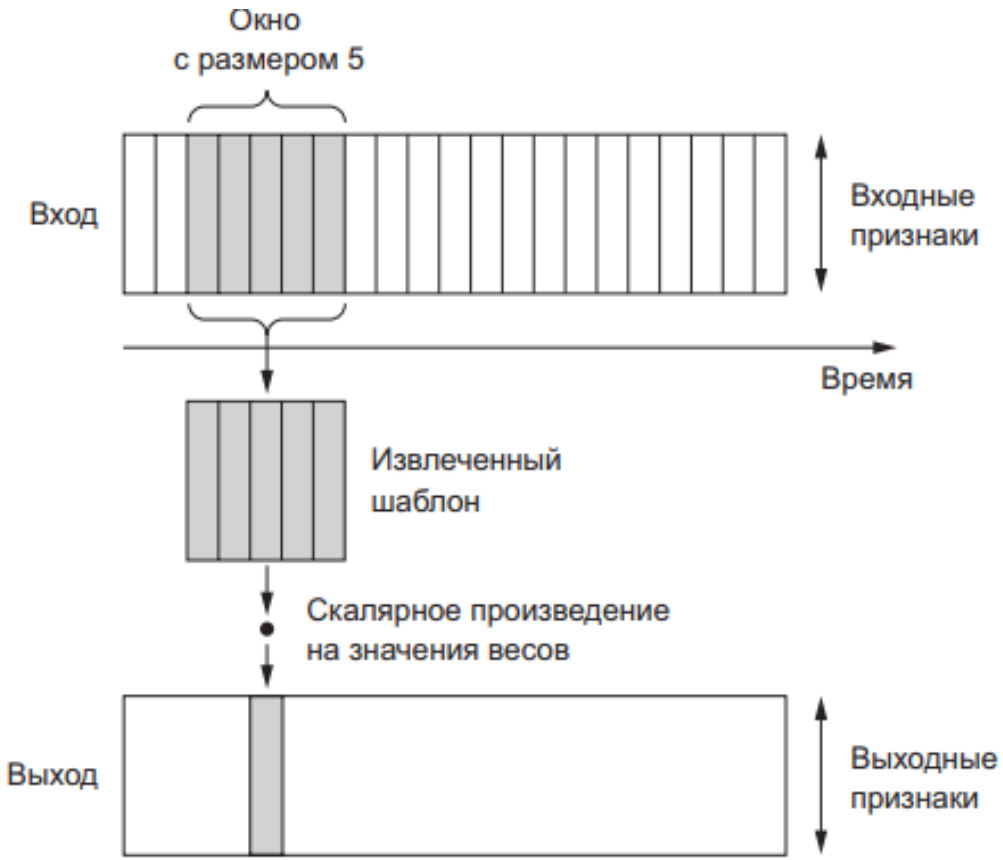
Сверточные нейронные сети/слои – операция субдискретизации или агрегации

- Операция субдискретизации (англ. subsampling, англ. pooling, также переводимая как «операция подвыборки» или операция объединения), выполняет уменьшение размерности сформированных карт признаков (только по ширине и высоте, а не по глубине) путем применения операций максимума или среднего из нескольких соседних нейронов карты. Распространенной формой пулинга является максимальный пулинг, в котором мы берем фильтр и применяем максимальную операцию **max** с определенной частью изображения. На рисунке показана операция MaxPooling2D с размером фильтра 2×2 и шагом 2. Выход представляет собой максимальное значение в области 2×2, показанной с использованием окруженных цифр.



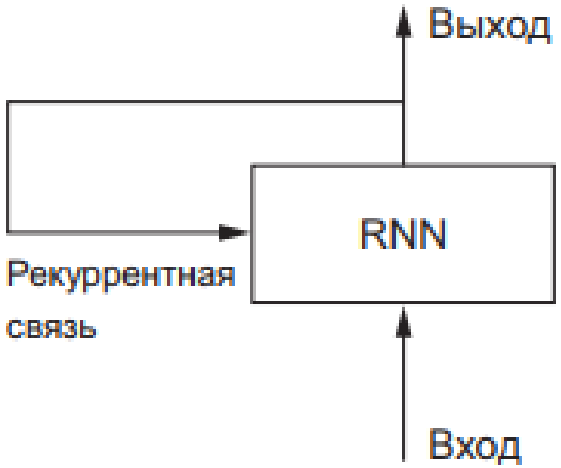
Сверточные нейронные сети/слои – одномерный вариант Conv1D

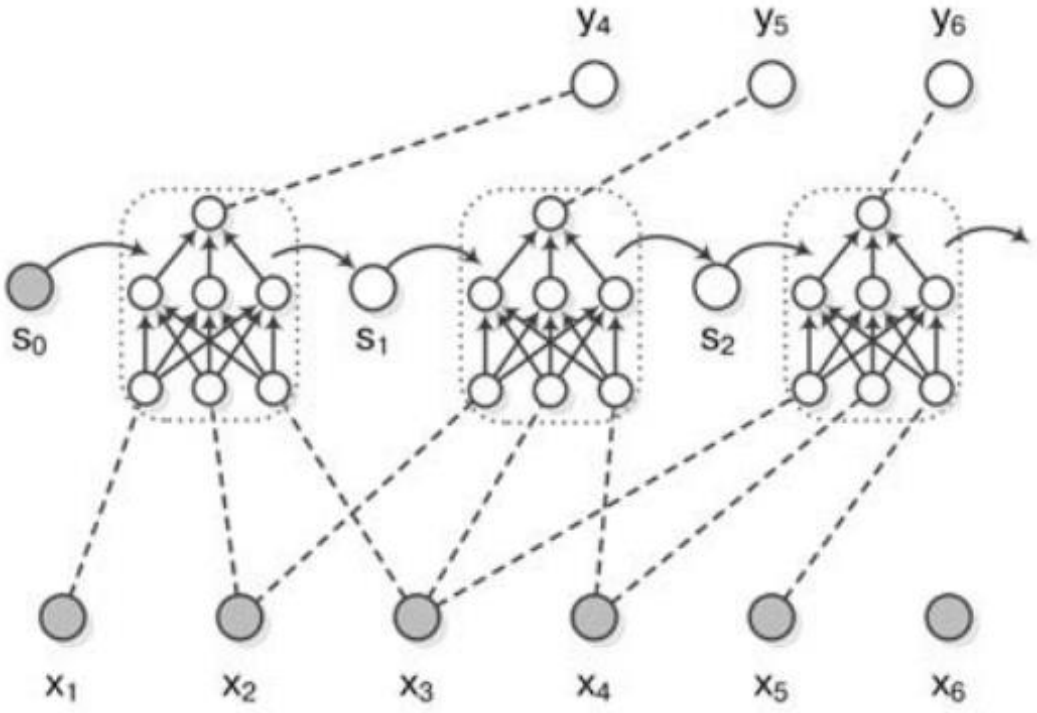
- Извлеченная сверткой информация, подается, как и в случае с полносвязной ИНС, на вход активационной функции a(Z). За блоком слоев 1D CNN должен следовать дискриминантный классификатор, который обычно является блоком полносвязных слоев. Ему может предшествовать операция агрегации (Pooling), которая также может присутствовать как промежуточный слой между блоками 1D CNN слоев. Pooling средний (AveragePooling) или максимальный (MaxPooling) принимает входной временной ряд и сокращает его длину T путем агрегирования в скользящем окне временного ряда.



Рекуррентные нейронные сети/слои

- *Рекуррентная нейронная сеть* (PHC, Recurrent Neural Network, RNN) обрабатывает последовательность, перебирая ее элементы и сохраняя *состояние*, полученное при обработке предыдущих элементов. Фактически RNN — это разновидность нейронной сети, имеющей внутренний цикл или обратную связь.

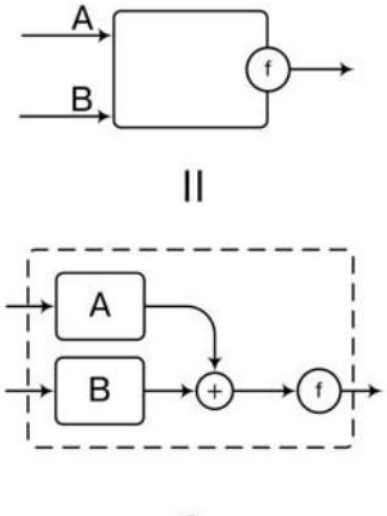


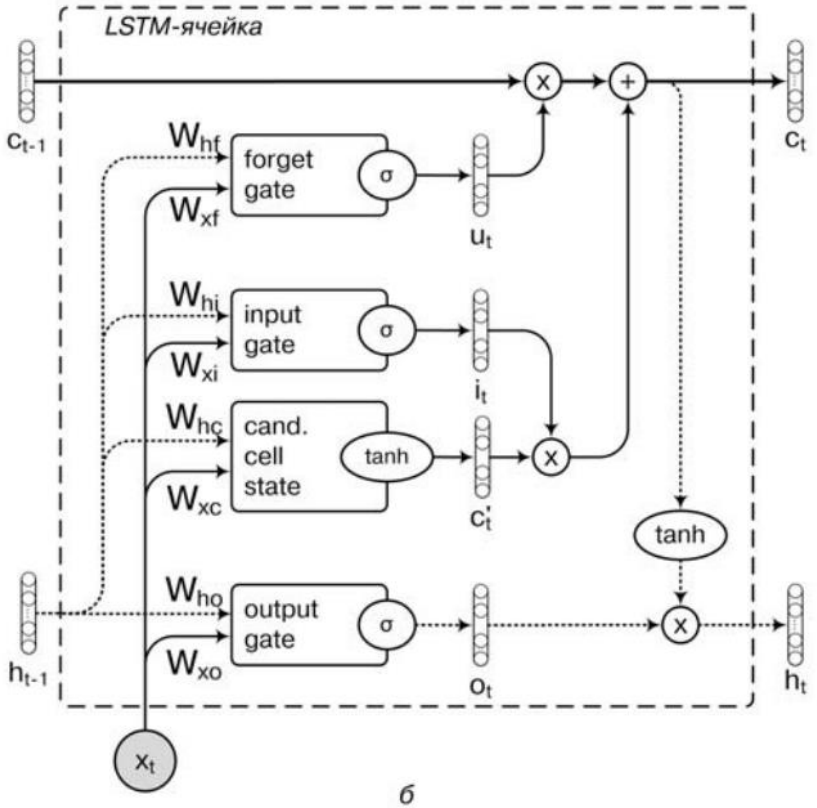


Рекуррентные нейронные сети/слои
Long Short-Term Memory-LSTM RNN

- Обычные RNN очень плохо справляются с ситуациями, когда нужно что-то «запомнить» надолго: влияние скрытого состояния или входа с шага *t* на последующие состояния рекуррентной сети экспоненциально затухает.
- Решения, которые на данный момент предлагаются, состоят главным образом в том, чтобы изменить, усложнить архитектуру одной ячейки – «кирпичика» рекуррентной сети. Одна из самых широко известных и часто применяющихся конструкций таких ячеек — это LSTM (от слов *Long Short-Term Memory* – длинная краткосрочная память).

$$
\begin{aligned}
\boldsymbol{c}'_t &= \tanh\left(W_{xc}\boldsymbol{x}_t + W_{hc}\boldsymbol{h}_{t-1} + \boldsymbol{b}_{c'}\right) && \textit{candidate cell state}\\
\boldsymbol{i}_t &= \sigma\left(W_{xi}\boldsymbol{x}_t + W_{hi}\boldsymbol{h}_{t-1} + \boldsymbol{b}_i\right) && \textit{input gate}\\
\boldsymbol{f}_t &= \sigma\left(W_{xf}\boldsymbol{x}_t + W_{hf}\boldsymbol{h}_{t-1} + \boldsymbol{b}_f\right) && \textit{forget gate}\\
\boldsymbol{o}_t &= \sigma\left(W_{xo}\boldsymbol{x}_t + W_{ho}\boldsymbol{h}_{t-1} + \boldsymbol{b}_o\right) && \textit{output gate}\\
\boldsymbol{c}_t &= \boldsymbol{f}_t \odot \boldsymbol{c}_{t-1} + \boldsymbol{i}_t \odot \boldsymbol{c}'_t, && \textit{cell state}\\
\boldsymbol{h}_t &= \boldsymbol{o}_t \odot \tanh(\boldsymbol{c}_t) && \textit{block output}
\end{aligned}
$$

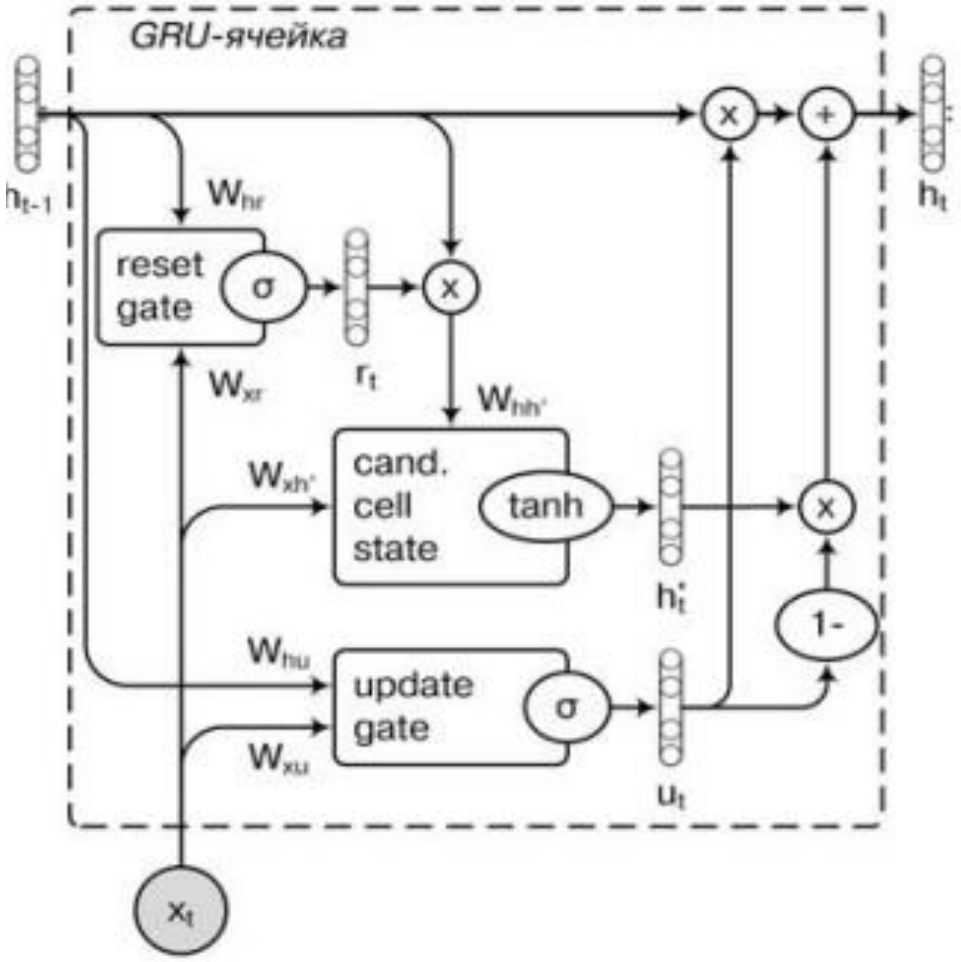




Рекуррентные нейронные сети/слои
Long Short-Term Memory-LSTM RNN

- В 2014 г. была предложена модификация LSTM рекуррентных сетей – Gated Recurrent Units (GRU), которая уменьшала сложность LSTM моделей и сокращала время обучения. В этой архитектуре скрытое состояние h_t совмещено со значением памяти c_t.

$$u_t = \sigma(W_{xu}x_t + W_{hu}h_{t-1} + b_u)$$
$$r_t = \sigma(W_{xr}x_t + W_{hr}h_{t-1} + b_r)$$
$$h'_t = \tanh(W_{xh'}x_t + W_{hh'}(r_t \circ h_{t-1}))$$
$$h_t = (1 - u_t) \circ h'_t + u_t \circ h_{t-1}.$$



Спектральный метод понижения размерности пространства данных на основе диффузионных карт

- Разработан спектральный метод понижения размерности пространства данных телеметрии МКА на основе диффузионных карт с Гауссовым (RBF) ядром, и нейросетевых моделей автокодировщика и полносвязных многослойных сетей, реализующих этапы кодирования и декодирования. При этом решаются следующие задачи:
- 1) понижения размерности исходного пространства данных телеметрической информации МКА поскольку мы получаем обученную нейросетевую модель, кодировщик которой реализует функцию диффузионной карты на построенной обучающей выборке для тестовых наборов или рабочих анализируемых данных;
- 2) установив порог среднеквадратичной ошибки, мы можем также определить для новых анализируемых данных их соответствие обученной модели и установить тем самым является ли точка данных выбросом, то есть точкой потенциально опасной нештатной ситуацией функционирования МКА;
- 3) шумоподавления, поскольку декодировщик, который реализует обратное отображение, может восстановить только гладкую версию данных тем самым ввод новых зашумленных векторов в автокодировщик дает на выходе очищенную от шумов версию векторов данных.