Научная статья

https://doi.org/10.54220/v.rsue.1991-0533.2025.92.4.021
УДК 330.4:004.94+004.032

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ПРОГНОЗИРОВАНИЯ КИБЕРАТАК НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Титов А. Ю.*[1]
[1] *Отдел информационной безопасности ООО «Радиус», Белгород, Россия*
** titov_a@voice-company.ru*

Аннотация. *Введение.* Современные условия развития цифровой экономики выдвигают новые требования, направленные на сохранение экономического суверенитета. Повышенный уровень кибератак побуждает перейти от реактивной к проактивной защите, построенной на применении математических методов и моделей. Интеграция таких моделей в национальные и корпоративные системы безопасности становится инвестицией в устойчивость экономики, защиту ВВП и поддержание общественного доверия к цифровым экосистемам. *Материалы и методы.* В данной статье рассматривается проблема прогнозирования фишинговых и DDoS-атак с использованием методов машинного обучения, в частности нейронных сетей. Автором предложена архитектура трехслойного перцептрона, который обучается на основе реальных данных о кибератаках. В работе исследуются различные функции активации, включая Relu, Tanh, Sigmoid, ELU для определения их влияния на эффективность модели. *Результаты исследования.* Проведена сравнительная оценка построенных моделей, демонстрирующая их производительность и точность в прогнозировании атак, что позволяет выделить наиболее эффективные подходы для защиты информационных систем. Результаты исследования могут быть полезны для специалистов в области кибербезопасности и разработки систем защиты от угроз. *Обсуждение и заключение.* Проведенные эксперименты показали, что каждая из функций активации имеет свои преимущества и недостатки, что позволяет выбрать наиболее подходящую в зависимости от конкретной задачи. В статье построены графики, на которых проведено сравнение исторических данных с прогнозными значениями, позволившие наглядно оценить качество предсказаний. На основе метрик MAE и MSE произведена оценка качества прогнозирования кибератак с помощью таких используемых в модели перцептрона активационных функций, как Relu, Tanh, Sigmoid, ELU. Данный подход позволяет провести количественную оценку прогнозных данных, что обеспечивает объективное сравнение эффективности моделей.

Ключевые слова: экономическая безопасность, кибербезопасность, прогнозирование, математические модели, нейронные сети.

Для цитирования: Титов А. Ю. Математические модели прогнозирования кибератак на основе искусственных нейронных сетей. *Вестник Ростовского государственного экономического университета (РИНХ).* 2025;4(32):241-252. DOI: 10.54220/v.rsue.1991-0533.2025.92.4.021.

Research article

JEL O38 G18 C53

MATHEMATICAL MODELS FOR PREDICTING CYBER-ATTACKS BASED ON ARTIFICIAL NEURAL NETWORKS

Titov A.*[1]
[1] *Information Security Department of Radius LLC, Belgorod, Russia*
* *titov_a@voice-company.ru*

Abstract. *Introduction.* Modern conditions of digital economy development put forward new requirements aimed at preserving economic sovereignty. The increased level of cyber-attacks encourages a transition from reactive to proactive protection based on the use of mathematical methods and models. Integrating such models into national and corporate security systems becomes an investment in economic resilience, protecting GDP and maintaining public trust in digital ecosystems. *Materials and methods.* This article examines the problem of predicting phishing and DDoS attacks using machine learning methods, in particular neural networks. The author proposes a three-layer perceptron architecture that is trained using real cyberattack data. The paper examines various activation functions, including Relu, Tanh, Sigmoid, ELU, to determine their impact on the model's efficiency. *Research results.* A comparative assessment of the constructed models was conducted, demonstrating their performance and accuracy in predicting attacks, which allows us to identify the most effective approaches for protecting information systems. The results of the study may be useful for specialists in the field of cybersecurity and development of threat protection systems. *Discussion and conclusion.* The experiments conducted showed that each of the activation functions has its own advantages and disadvantages, which allows you to choose the most suitable one depending on the specific task. The article contains graphs that compare historical data with forecast values, allowing for a clear assessment of the quality of the predictions. Based on the MAE and MSE metrics, the quality of forecasting cyber-attacks was assessed using the activation functions used in the perceptron model, such as Relu, Tanh, Sigmoid, ELU. This approach allows for a quantitative assessment of forecast data, which ensures an objective comparison of the effectiveness of models.

Keywords: economic security, cybersecurity, forecasting, mathematical models, neural networks.

For citation: Titov A. Mathematical Models for Predicting Cyber-Attacks Based on Artificial Neural Networks. *Vestnik of Rostov State University of Economics (RINH).* 2025;4(32): 241-252. DOI: 10.54220/v.rsue.1991-0533.2025.92.4.021.

Введение

В эпоху цифровизации, когда экономические процессы неразрывно связаны с киберпространством, устойчивость национальных и корпоративных систем напрямую зависит от способности предвидеть и нейтрализовать киберугрозы. В связи с тем, что в последние годы происходит постоянное наращивание сложности кибератак, они создают значительную опасность для экономики любой страны. Поэтому решение вопросов информационной безопасности становится наиболее важной и актуальной проблемой управления хозяйствующими субъектами, так как количество и изощренность кибератак постоянно растут. Их воздействия создают значительные проблемы как для частных компаний, так и для государств из-за утечки информации, финансовых потерь

и др. Все это свидетельствует о том, что разработка и применение действенных методов прогнозирования кибератак с целью дальнейшего их предотвращения является ключевой проблемой информационной безопасности. В связи с этим в настоящее время в научной литературе все чаще появляются публикации, в которых отражаются вопросы прогнозирования и предотвращения киберугроз. Увеличение частоты и сложности киберугроз требует разработки эффективных методов защиты, что, в свою очередь, стимулирует исследователей к поиску инновационных подходов и решений. Так, в работе [1] предложен эффективный алгоритм обработки данных на основе фильтра Калмана, который убирает шумы и лишнюю информацию в ходе предсказания состояния системы. Авторами проведено исследование возможности применения фильтра Каллмана для решения задачи прогнозирования временных рядов. В статье [2] проведено исследование возможностей и ограничений использования методов теории временных рядов для анализа и прогнозирования динамики кибератак на примере ведомственного вуза. Статья [3] посвящена созданию автоматизированной информационной системы оценки и прогнозирования киберугроз на морских судах. Системный подход к разработке математического обеспечения систем обнаружения кибератак и прогнозирования работоспособности информационной системы предложен в работе [4]. Авторами описан комплекс моделей, позволяющих принимать диагностические решения о состоянии работоспособности программного обеспечения. Применению математического аппарата нечеткой логики и созданию на его основе моделей обеспечения информационной безопасности посвящены исследования [5, 6, 7, 8, 9]. Среди множества подходов, применяемых для анализа и предсказания киберугроз, особое место занимают методы, основанные на искусственных нейронных сетях. Эти методы способны обрабатывать большие объемы данных и выявлять сложные закономерности, что делает их эффективными инструментами в борьбе с киберпреступностью. Этот факт стал причиной роста числа исследований, результаты которых отражены в научных публикациях. В частности, в работе [10] представлена модель безопасности для когнитивных информационных центров с использованием метода, сочетающего в себе нейронные сети и генетические алгоритмы. Модель использует нейросетевую эволюцию для создания адаптируемых моделей, способных обучаться в ответ на широкий спектр киберугроз. Основные проблемы, связанные с угрозой DDoS-атак, рассматриваются в работах [11, 12]. Исследование охватывает различные аспекты защиты информации, включая обнаружение и классификацию DDoS-атак, анализ трафика, а также прогнозирование и предотвращение возможных атак.

Представленная статья посвящена исследованию математических моделей, основанных на искусственных нейронных сетях, для прогнозирования фишинговых и DDoS-атак. Рассматриваются вопросы применения различных функций активации в многослойном перцептроне, а также проведен сравнительный анализ их эффективности на примере реальных данных. Целью работы является выявление наиболее подходящих моделей для различных типов атак, что позволит улучшить стратегии защиты и повысить уровень безопасности в цифровом пространстве.

Материалы и методы

В данной работе для прогнозирования кибератак по историческим данным предлагается модель искусственной нейронной сети в виде многослойного перцептрона. Архитектура сети включает входной и выходной слои с двумя нейронами, что соответствует двум типам атак: фишинговым и DDoS-атакам. Между ними расположены три скрытых слоя с количеством нейронов, равным 128, 64, 32 нейрона в каждом слое соответственно. Архитектура нейронной сети приведена на рисунке 1.

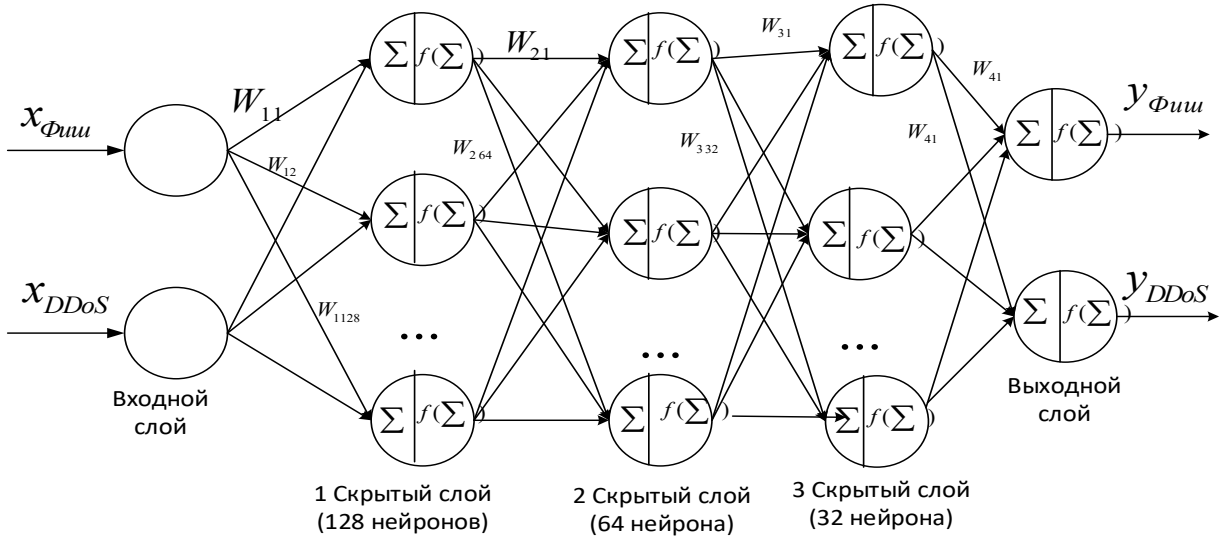

Рисунок 1 − **Архитектура нейронной сети прогнозирования кибератак**
Figure 1 − **Architecture of a neural network for predicting cyber attacks**

Каждый нейрон слоя вычисляет значение z_{ij} функции активации f от взвешенной суммы $z_{ij} = f(\sum_{j=1}^{n} W_{i-1,j}\ j \cdot z_{i-1\,j})$, где i – номер слоя, j – номер нейрона в слое. Для повышения качества прогнозирования в модели многослойного перцептрона используются различные функции активации, среди которых ReLU (Rectified Linear Unit), Tanh (Hyperbolic Tangent), Sigmoid (сигмоидальная функция) и ELU (Ecsponential Linear Unit). Каждая из этих функций имеет свои преимущества и недостатки. Их применение будет варьироваться в зависимости от специфики данных и решаемой задачи.

Опишем эти функции. ReLU (Rectified Linear Unit), линейная функция активации с обрезкой, описывается математически как $f(x) = \max(0, x)$. Эта функция возвращает ноль для всех отрицательных значений и само значение для положительных значений. Функция Tanh (Hyperbolic Tangent), гиперболический тангенс, представляется формулой $f(x) = \tanh(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}}$. Он преобразует входные данные в диапазон [-1,1]. Sigmoid (Logistic Function), сигмоидальная функция, возвращает значения в диапазоне [0,1] и задается математически уравнением $f(x) = \delta(x) = \frac{1}{1 + e^{-x}}$. ELU (Ecsponential Linear Unit), экспоненциальная линейная единица, формализуется с помощью математического выражения $f(x) = \begin{cases} x & если\ x \geq 0 \\ \alpha(e^{x} - 1) & если\ x < 0 \end{cases}$. Эта функция похожа на ReLU, но для отрицательных значений возвращает экспоненциальную часть, что помогает избежать проблему «мертвых нейронов».

Графики функций ReLU, Tanh, Sigmoid, ELU приведены на рисунке 2. Характеризуя применяемые в модели нейронной сети функции активации, следует заключить следующее. Функция активации ReLU в модели многослойного перцептрона позволяет решить проблему исчезающего градиента, что дает возможность ускорить процесс обучения. Функция Tanh обладает свойством быстрой сходимости. Хотя функция Sigmoid является менее предпочтительной для глубоких сетей, она может быть полезна для бинарной классификации.

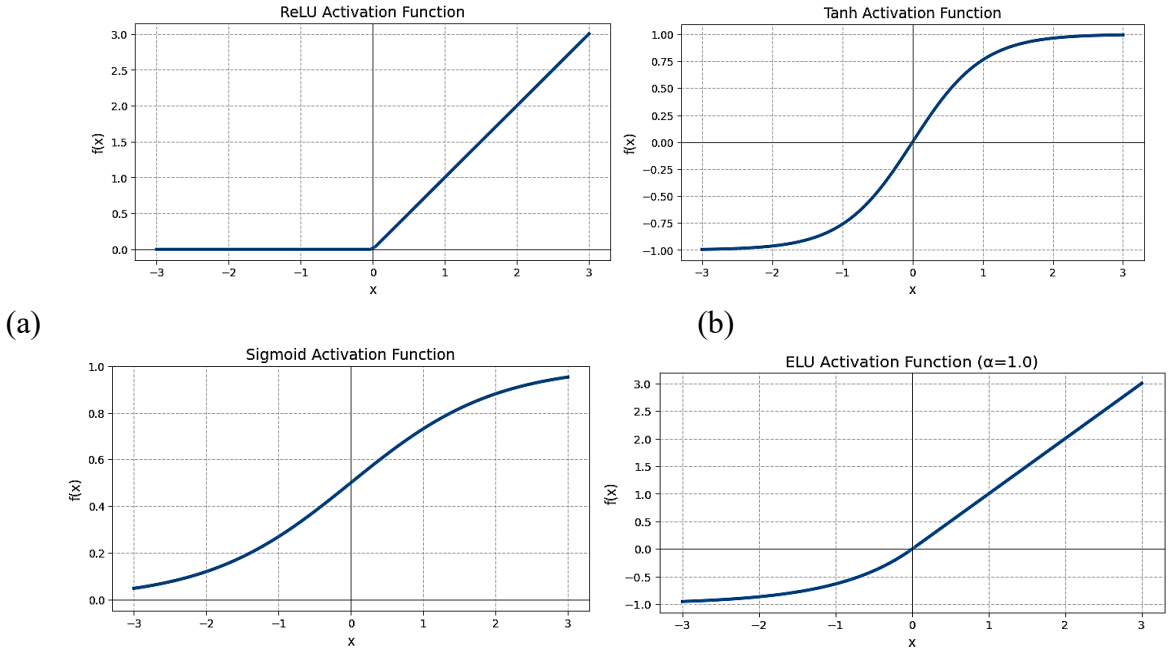

Рисунок 2 − **Графики функций активации: (a) функции ReLU (Rectified Linear Unit); (b) Tanh (Hyperbolic Tangent); (c) Sigmoid (Logistic Function); (d) ELU (Ecsponential Linear Unit)**

Figure 2 − **Graphs of activation functions: (a) functions ReLU (Rectified Linear Unit); (b) Tanh (Hyperbolic Tangent); (c) Sigmoid (Logistic Function); (d) ELU (Ecsponential Linear Unit)**

Активационная функция ELU может быть продуктивной из-за включенной в нее экспоненциальной составляющей, благодаря которой улучшается сходимость обучения. На простроенной модели многослойного перцептрона проведены эксперименты с различными функциями активации. Для оценки эффективности применения этих функций используются метрики MAE (Mean Absolute Error) и MSE (Mean Square Error). Метрика MAE, среднеквадратическая абсолютная ошибка, описывается математическим выражением

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|,$$

где y_i – реальное значение; $\hat{y}_i$ – предсказанное значение; n – количество наблюдений. Особенности метрики: измеряется в тех же единицах, что и исходные данные; не учитывает направление ошибки (только абсолютную величину); менее чувствительна к выбросам. Метрика MSE, среднеквадратическая ошибка, формально представляется как

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$$

Особенности метрики: измеряется в квадратах единиц исходных данных; сильно штрафуется за большие ошибки (из-за возведения в квадрат); используется как функция потерь при обучении нейросетей.

Далее представим результаты экспериментов, проведенных на модели построенного трехслойного перцептрона с использованием реальных исторических данных.

Результаты исследования

Для проведения экспериментов с использованием построенного трехслойного перцептрона были собраны ежемесячные данные о количестве кибератак (фишинг и DDoS) за период с января 2020 г. по февраль 2024 г. (табл. 1).

Таблица 1 – **Ежемесячные данные о количестве кибератак (фишинг и DDoS) за период с января 2020 г. по февраль 2024 г.**
Table 1 − **Monthly data on the number of cyberattacks (phishing and DDoS) for the period from January 2020 to February 2024**

Месяц	Фишинг	DDoS	Месяц	Фишинг	DDoS
2020-01-31	4200	2100	2022-01-31	14 000	9800
2020-02-29	4500	2300	2022-02-28	14 500	10 300
2020-03-31	5000	2800	2022-03-31	15 200	11 000
2020-04-30	5400	3000	2022-04-30	15 800	11 500
2020-05-31	5800	3200	2022-05-31	16 500	12 000
2020-06-30	6200	3500	2022-06-30	17 200	12 800
2020-07-31	6600	3800	2022-07-31	17 900	13 500
2020-08-31	5900	3600	2022-08-31	17 500	13 200
2020-09-30	6800	4000	2022-09-30	18 500	14 000
2021-05-31	10 500	6500	2023-05-31	25 600	21 000
2021-06-30	11 000	7000	2023-06-30	26 800	22 000
2021-07-31	11 500	7500	2023-07-31	28 000	23 000
2021-08-31	11 200	7200	2023-08-31	27 500	22 800
2021-09-30	12 000	7800	2023-09-30	29 000	24 000
2021-10-31	12 500	8300	2023-10-31	30 500	25 200
2021-11-30	13 000	8800	2023-11-30	32 000	26 500
2021-12-31	13 500	9300	2024-02-29	36 500	30 200

Из-за ограниченности объема статьи в таблице 1 приведена только часть исторических данных о количестве кибератак. Но в проведении экспериментов участвовали все исторические данные.

Далее в статье представим результаты прогнозирования кибератак с использованием различных функций активации.

Прогноз кибератак с использованием функции активации RELU

На рисунке 3 приведены результаты прогнозирования фишинговых и DDoS-атак при использовании функции ReLU ((Rectified Linear Unit) – линейной функции активации. В таблице 2 представлены результаты прогноза кибератак моделью перцептрона, построенного на применении функции активации ReLU.

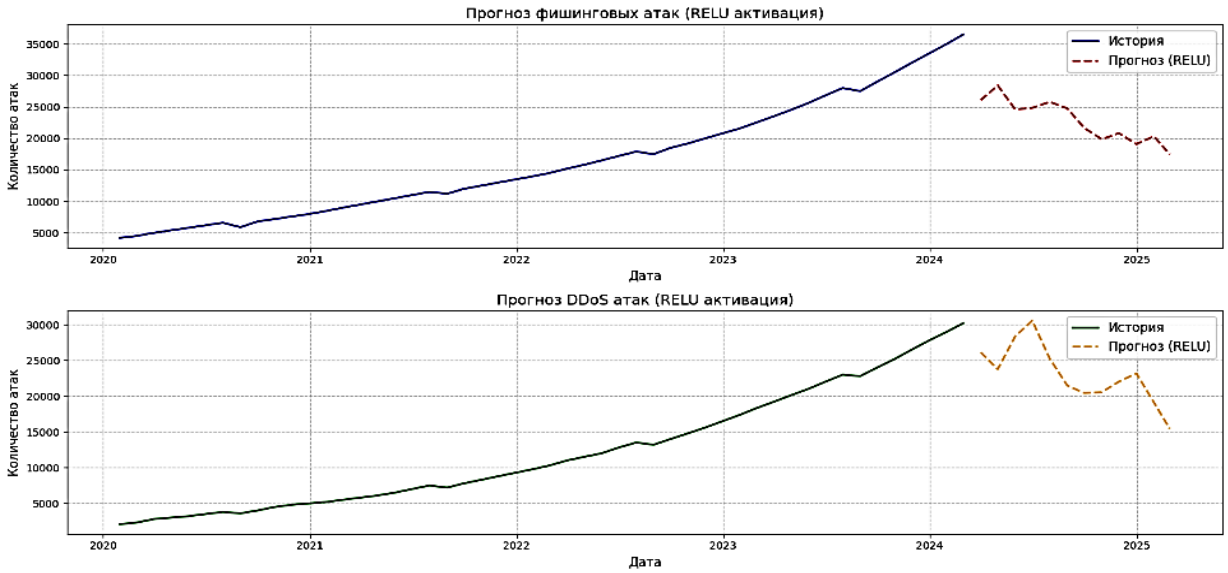

Рисунок 3 − **Прогноз фишинговых и DDoS-атак с функцией активации ReLU**
Figure 3 − **Prediction of phishing and DDoS attacks with ReLU activation function**

Таблица 2 – **Результаты прогноза кибератак на 12 месяцев моделью перцептрона, построенного на применении функции активации ReLU**
Table 2 – **Results of forecasting cyber-attacks for 12 months using a perceptron model built on the ReLU activation function**

Дата	Фишинг	DDoS
2024-03-31	26 076	26 130
2024-04-30	28 406	23 765
2024-05-31	24 602	28 379
2024-06-30	24 840	30 562
2024-07-31	25 794	25 239
2024-08-31	24 754	21 478
2024-09-30	21 653	20 434
2024-10-31	19 864	20 563
2024-11-30	20 824	22 022
2024-12-31	19 101	23 190
2025-01-31	20 323	19 117
2025-02-28	17 474	15 428

Прогноз кибератак с использованием функции активации TANH

На рисунке 4 проиллюстрированы результаты прогнозирования фишинговых и DDoS-атак при использовании в модели перцептрона активационной функции TANH (Hyperbolic Tangent) – гиперболического тангенса. Количественные значения прогноза на 12 месяцев приведены в таблице 3.

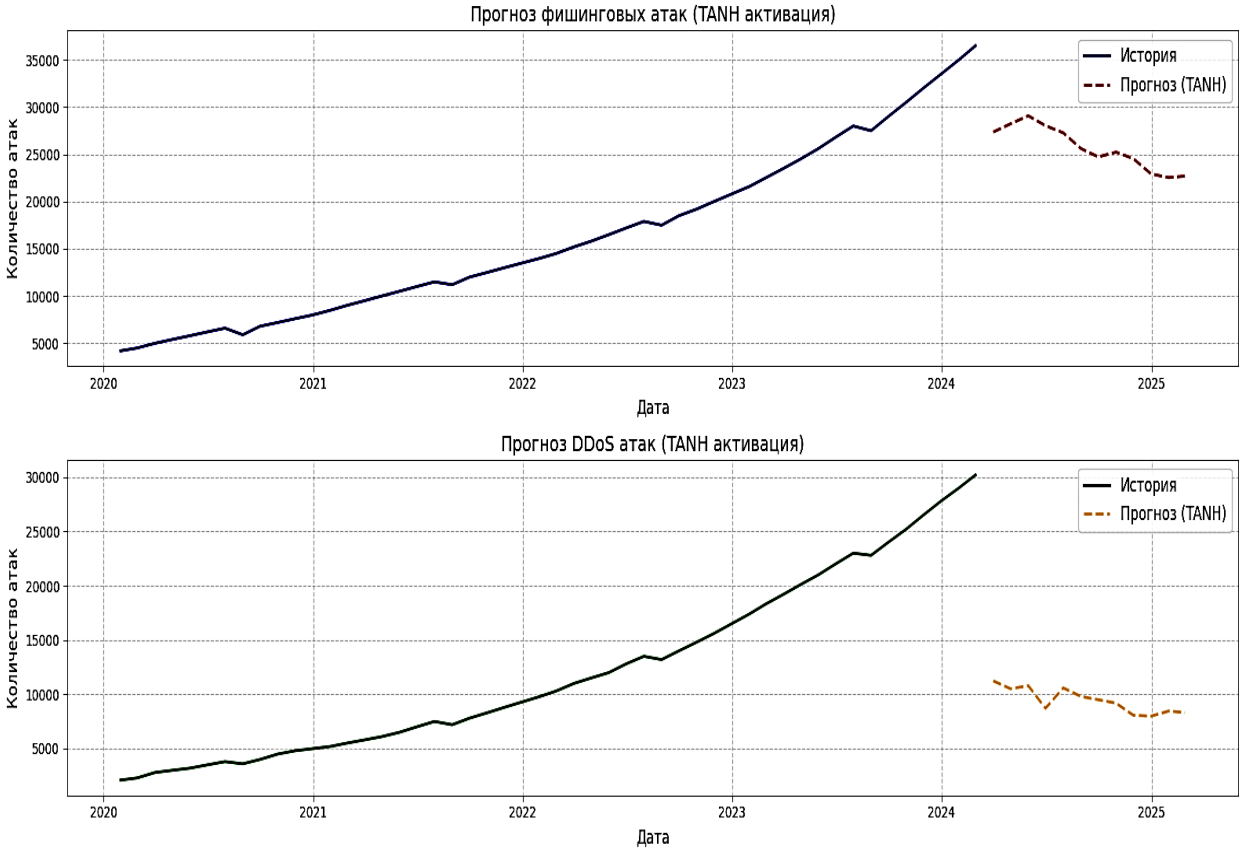

Рисунок 4 − **Прогноз фишинговых и DDoS-атак с функцией активации TANH**
Figure 4 − **Forecasting phishing and DDoS attacks with TANH activation function**

Таблица 3 – **Результаты прогноза кибератак на 12 месяцев моделью перцептрона, построенного на применении функции активации TANH**
Table 3 – **Results of forecasting cyber-attacks for 12 months using a perceptron model built on the application of the TANH activation function**

Дата	Фишинг	DDoS
2024-03-31	27 361	11 236
2024-04-30	28 232	10 512
2024-05-31	29 080	10 789
2024-06-30	28 036	8714
2024-07-31	27 272	10 589
2024-08-31	25 606	9797
2024-09-30	24 729	9504
2024-10-31	25 234	9185
2024-11-30	24 548	8074
2024-12-31	22 928	7988
2025-01-31	22 538	8461
2025-02-28	22 694	8317

Прогноз кибератак с использованием функции активации SIGMOID

Рисунок 5 демонстрирует результат прогнозирования фишинговых и DDoS-атак моделью нейронной сети с применением сигмоидальной функции активации. Таблица 4 показывает количественные значения результатов прогноза.

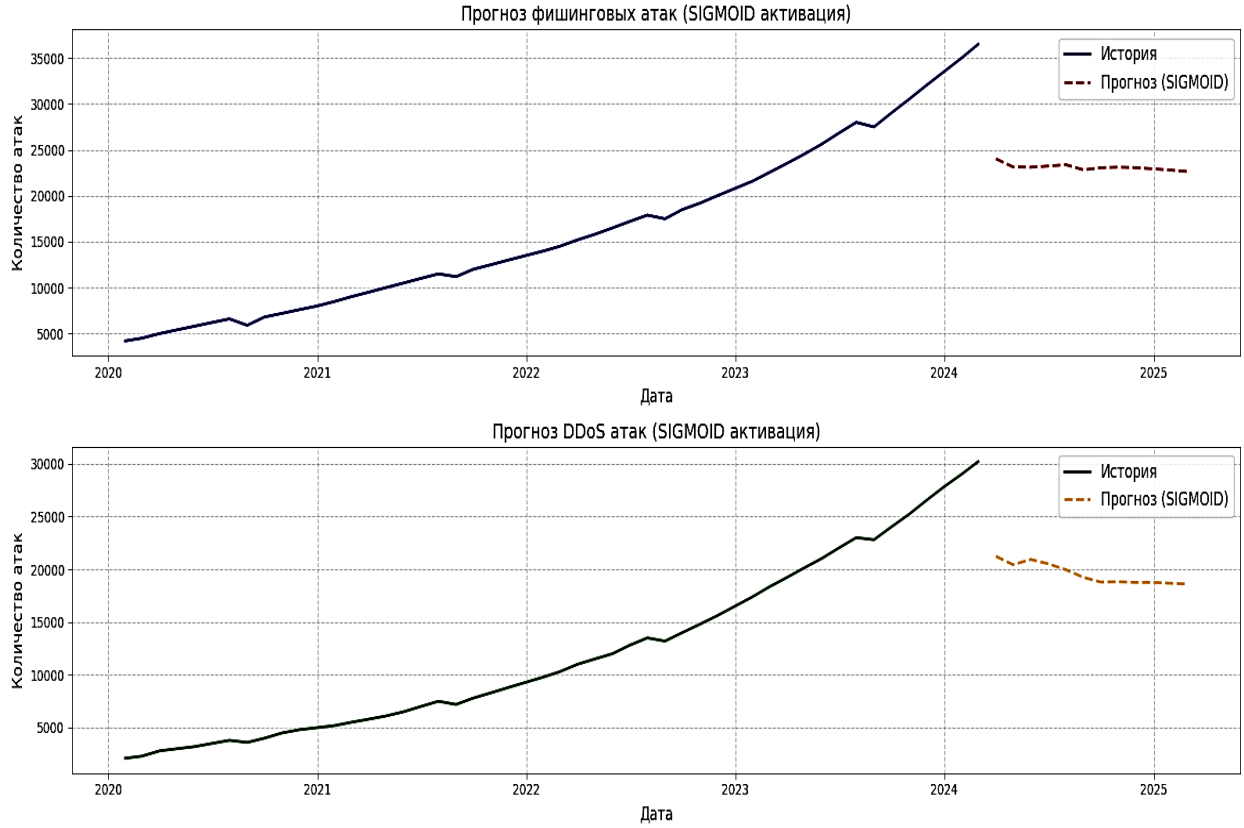

Рисунок 5 − **Прогноз фишинговых и DDoS атак с функцией активации SIGMOID**
Figure 5 − **Forecasting phishing and DDoS attacks with SIGMOID activation function**

Таблица 4 – **Результаты прогноза кибератак на 12 месяцев моделью перцептрона, построенного на применении функции активации SIGMOID**
Table 4 – **Results of forecasting cyber-attacks for 12 months using a perceptron model built on the application of the SIGMOID activation function**

Дата	Фишинг	DDoS
2024-03-31	24 034	21 230
2024-04-30	23 143	20 434
2024-05-31	23 114	20 934
2024-06-30	23 240	20 525
2024-07-31	23 390	19 969
2024-08-31	22 826	19 233
2024-09-30	23 059	18 792
2024-10-31	23 121	18 817
2024-11-30	23 068	18 761
2024-12-31	22 937	18 754
2025-01-31	22 795	18 678
2025-02-28	22 649	18 603

Прогноз кибератак с использованием функции активации ELU

Рисунок 6 демонстрирует результат прогнозирования фишинговых и DDoS-атак моделью нейронной сети с применением сигмоидальной функции активации (Ecsponential Linear Unit) – экспоненциальной линейной единицы. Количественные результаты прогноза приведены в таблице 5.

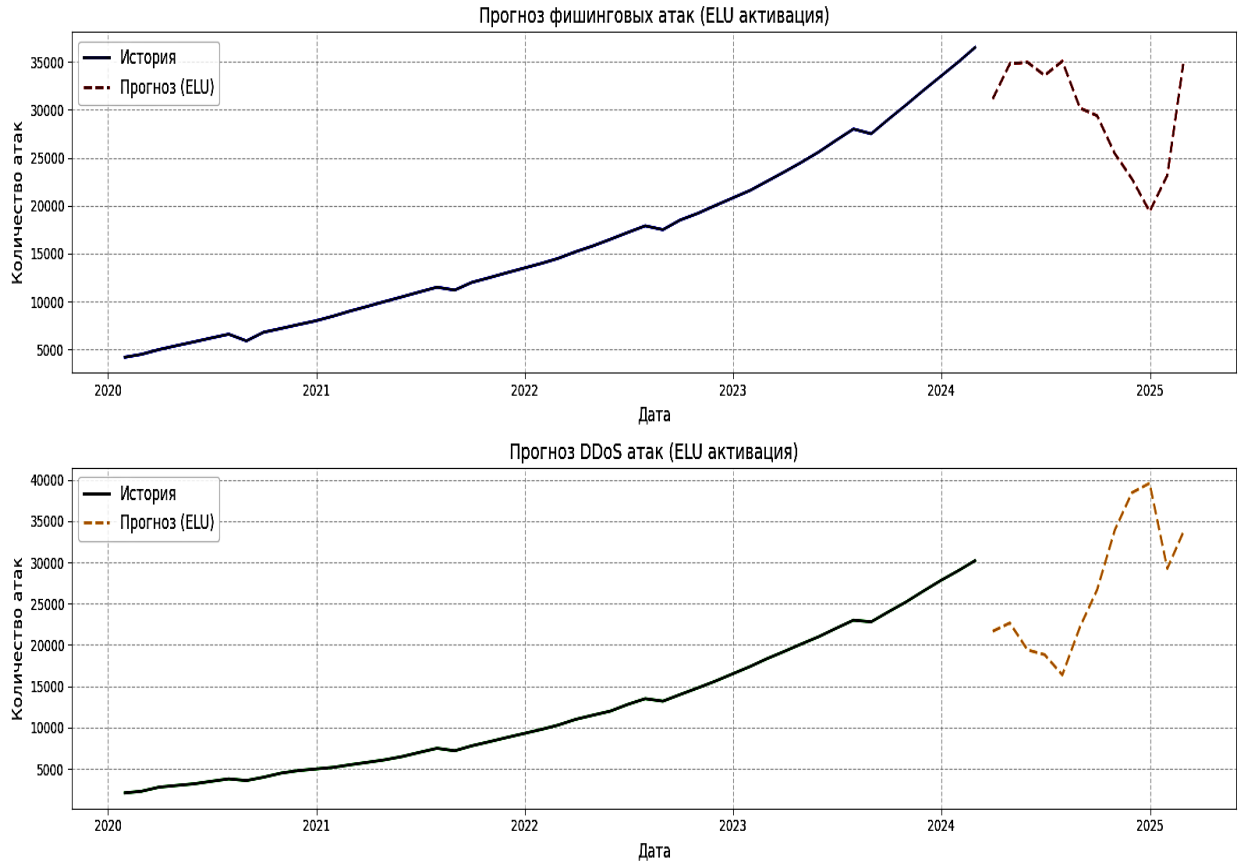

Рисунок 6 – **Прогноз фишинговых и DDoS атак с функцией активации ELU**
Figure 6 – **Phishing and DDoS attack prediction with ELU activation function**

Таблица 5 – **Результаты прогноза кибератак на 12 месяцев моделью перцептрона, построенного на применении функции активации ELU**
Table 5 – **Results of forecasting cyber-attacks for 12 months using a perceptron model built on the application of the ELU activation function**

Дата	Фишинг	DDoS
2024-03-31	31 138	21 656
2024-04-30	34 805	22 661
2024-05-31	34 955	19 403
2024-06-30	33 591	18 826
2024-07-31	35 073	16 377
2024-08-31	30 179	22 191
2024-09-30	29 388	26 679
2024-10-31	25 425	33 904
2024-11-30	22 810	38 421
2024-12-31	19 398	39 568
2025-01-31	23 163	29 250
2025-02-28	34 793	33 640

Обсуждение и заключение

Оценка эффективности моделей нейронной сети с различными функциями активации произведена с помощью метрик MAE и MSE (табл. 6).

Таблица 6 – **Оценка эффективности моделей нейронной сети с различными функциями активации**
Table 6 – **Evaluation of the effectiveness of neural network models with different activation functions**

Активация	MSE Фишинг	MAE Фишинг	Точность Фишинг, %	MSE DDoS	MAE DDoS	Точность DDoS, %
RELU	47423418,30	6429,12	79,83	19920206,02	4346,37	82,59
TANH	21661575,45	3430,17	89,84	240811131,10	15349,77	40,32
SIGMOID	63513188,85	7395,23	76,86	30010107,66	4947,89	81,43
ELU	12634971,64	3352,12	89,16	36217491,86	5432,38	79,61

В результате оценки эффективности построенной нейронной сети следует заключить, что для обнаружения фишинговых атак наиболее эффективно использовать функцию активации TANH, которая продемонстрировала точность 89,84 %). В то же время для выявления DDoS-атак предпочтительнее применять функцию RELU, обеспечивающую точность 82,59.

Как показывают публикации, в последние годы искусственные нейронные сети зарекомендовали себя как мощный инструмент для прогнозирования различных кибератак. Их способность обучаться на основе исторических данных делает их особенно полезными для прогнозирования различных типов кибератак. В данной статье представлены результаты разработки математической модели для прогнозирования фишинговых и DDoS-атак с использованием трехслойного перцептрона. Рассмотрены различные функции активации, такие как ReLU, Tanh, Sigmoid, ELU и проведена сравнительная оценка их эффективности на основе реальных данных. Проведенные эксперименты показали, что каждая из функций активации имеет свои преимущества и недостатки, что позволяет выбрать наиболее подходящую в зависимости от конкретной задачи. Для визуализации результатов исследований в статье построены

графики, на которых проведено сравнение исторических данных с прогнозными значениями, что позволяет наглядно оценить качество предсказаний. При использовании метрики MAE и MSE автором статьи произведена оценка качества прогнозирования кибератак с помощью используемых в модели перцептрона активационных функций ReLU, Tanh, Sigmoid, ELU. Это дало возможность дать количественную оценку полученных прогнозов.

Проведенное исследование свидетельствует о том, что нейронные сети в виде трехслойных перцептронов могут быть полезными для прогнозирования фишинговых и DDoS-атак. В дальнейшем планируется проведение исследований в области прогнозирования киберугроз на основе нейронных сетей, имеющих более сложную архитектуру.

Список литературы

1. Прогнозирование кибератак на промышленные системы с использованием фильтра Калмана / Д. П. Зегжда, Д. С. Лаврова, А. В. Ярмак // Проблемы информационной безопасности. Компьютерные системы. – 2019. – №. 2. – С. 164-171.

2. *Наумов, В. Н.* Анализ и прогнозирование временных рядов кибератак на информационную систему ведомственного вуза: возможности и ограничения методов // Труды учебных заведений связи. – 2025. – Т. 11, №. 1. – С. 99-112.

3. *Когтев, А. В.* Автоматизированная информационная система оценки и прогнозирования киберугроз на морских судах под флагом Российской Федерации: от субъектов киберугроз до этапов кибератаки // Нефтегазовые технологии и экологическая безопасность. – 2021. – № 2 (72). – С. 35-42.

4. *Душкин, А. В., Кочедыков, С. С.* Алгоритм прогнозирования работоспособности информационной системы после воздействия кибератак // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации. – 2020. – С. 142-148.

5. Mathematical Modeling of Fiscal Innovations Based on the Interdisciplinary Synthesis of Fuzzy Logic and Automata Theory / A. Abbasov, E. Streltsova, I. Yakovenko, A. Bogomyagkov // Azerbaijan Journal of Mathematics. – 2022. – Vol. 12, Issue 2. – P. 3-29.

6. Fuzzy-Logic Model for Feasibility Study of Project Implementation: Project's Investment Risk / E. Streltsova, A. Borodin, I. Yakovenko // Iranian Journal of Fuzzy Systems. – 2022. – Vol. 19, № 2. – P. 1-15.

7. Fuzzy-Logical Model for Analysis of Sustainable Development of Fuel and Energy Complex Enterprises / A. Borodin, E. Streltsova, Z. Mamedov, I. Yakovenko, I. Mityushina / AIMS Energy. – 2023. – Vol. 11, Issue 5. – P. 974-990.

8. Постановка задачи моделирования оценки информационной безопасности / Е. Д. Стрельцова, А. Ю. Титов, И. В. Яковенко // Друкеровский вестник. – 2024. – № 6. – С. 241-247.

9. Математическая модель оценки информационной безопасности хозяйствующих субъектов / Е. Д. Стрельцова, А. Ю. Титов, И. В. Яковенко // Друкеровский вестник. – 2024. – № 2. – С. 182-193

10. *Панилов, П. А.* Использование методов нейроэволюции для автоматизации оптимизации алгоритмов киберзащиты в когнитивных информационных центрах // Известия тульского государственного университета. технические науки. – 2024. – № 11. – С. 16-25.

11. *Пирлиев, К.* Эффективные подходы к обнаружению и предсказанию ddos-атак с использованием машинного обучения // Всемирный ученый. – 2024. – Т. 1, № 24. – С. 160-166.

12. *Яцкевич, Е. С.* Систематический анализ базовых методов нейросетевой защиты информации от DDoS-атак // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2024. – № 4 (351). – С. 38-45.

References

1. Forecasting Cyberattacks on Industrial Systems Using the Kalman Filter / D. Zegzhda, D. Lavrova, A. Yarmak // Problems of Information Security. Computer Systems. – 2019. – № 2. – P. 164-171.

2. *Naumov, V.* Analysis and Forecasting of Time Series of Cyber-Attacks on the Information System of a Departmental University: Capabilities and Limitations of Methods // Works of Educational Institutions of Communication. – 2025. – Vol. 11, № 1. – P. 99-112.

3. *Kogtev, A.* Automated Information System for Assessing and Forecasting Cyber Threats on Sea Vessels Under the Flag of Russian Federation: from Cyber Threat Subjects to Cyber-Attack Stages // Oil and Gas Technologies and Environmental Safety. – 2021. – № 2 (72). – P. 35-42.

4. *Dushkin A., Kochedykov, S.* Algorithm for Predicting the Operability of an Information System after Exposure to Cyberattacks // Fundamental Problems of Information Security in the Context of Digital Transformation. – 2020. – P. 142-148.

5. Mathematical Modeling of Fiscal Innovations Based on the Interdisciplinary Synthesis of Fuzzy Logic and Automata Theory / A. Abbasov, E. Streltsova, I. Yakovenko, A. Bogomyagkov // Azerbaijan Journal of Mathematics. – 2022. – Vol. 12, Issue 2. – P. 3-29.

6. Fuzzy-Logic Model for Feasibility Study of Project Implementation: Project's Investment Risk / E. Streltsova, A. Borodin, I. Yakovenko // Iranian Journal of Fuzzy Systems. – 2022. – Vol. 19, № 2. – P. 1-15.

7. Fuzzy-Logical Model for Analysis of Sustainable Development of Fuel and Energy Complex Enterprises / A. Borodin, E. Streltsova, Z. Mamedov, I. Yakovenko, I. Mityushina / AIMS Energy. – 2023. – Vol. 11, Issue 5. – P. 974-990.

8. Statement of the Problem of Modeling Information Security Assessment / E. Streltsova, A. Titov, I. Yakovenko // Drucker Bulletin. – 2024. – № 6. – P. 241-247

9. Mathematical Model for Assessing Information Security of Economic Entities / E. Streltsova, A. Titov, I. Yakovenko // Drucker Bulletin. – 2024. – № 2. – P. 182-193.

10. *Panilov, P.* Using Neuroevolution Methods to Automate the Optimization of Cyber Defense Algorithms in Cognitive Information Centers // Bulletin of Tula State University. Technical sciences. – 2024. – № 11. – P. 16-25.

11. *Pirliev, K.* Effective Approaches to Detecting and Predicting DDoS Attacks Using Machine Learning // World Scientist. – 2024. – Vol. 1. – № 24. – P. 160-166.

12. *Yatskevich, E.* Systematic Analysis of Basic Methods of Neural Network Protection of Information from DDoS Attacks // Bulletin of Adyghe State University. Series 4: Natural, Mathematical and Technical Sciences. – 2024. – № 4 (351). – P. 38-45.

Об авторах

Титов Александр Юрьевич, *руководитель отдела информационной безопасности ООО «Радиус», Белгород, Россия, titov_a@voice-company.ru.*

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

About the Authors

Alexander Titov, *Head of the Information Security Department of Radius LLC, Belgorod, Russia, titov_a@voice-company.ru.*

Conflict of Interest: The author declares no conflict of interest.