**УДК 004.8**

# НЕЙРОСЕТЕВОЕ ПРОГНОЗИРОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Беляева Т.А.[1], Микрюков А.А.[1]**

*[1] Российский экономический университет имени Г.В.Плеханова, e-mail: tanbel03@mail.ru*

**Аннотация**

**Данная работа содержит описание возможностей использования нейросетей в качестве эффективного инструмента обеспечения информационной безопасности. В контексте быстро меняющейся кибер среды, использование нейросетей не только усиливает защиту от новых угроз и атак, но и создает устойчивую основу для разработки адаптивных стратегий безопасности. Актуальность данного исследования обусловлена возрастающей распространенностью внедрений технологий искусственного интеллекта в различные сферы. Представленное решение задач прогнозирования инцидентов с помощью языка Python и библиотеки scikit-learn позволяет повысить надежность защиты, предупреждая появление большого количество новых угроз и атак, что также позволяет оценить эффективность мер безопасности, оптимизировать распределение ресурсов и планировать стратегии безопасности. Кроме того, статистика предоставляет базу для обучения систем искусственного интеллекта в области информационной безопасности, что способствует более точному прогнозированию и адаптации к изменяющимся угрозам, а также дает возможность проведения анализа в реальном времени. Такой комплексный подход предоставляет организациям инструментарий для оптимизации распределения ресурсов, планирования стратегий безопасности и повышения эффективности общей системы защиты. В работе, помимо этого, обсуждаются потенциальные проблемы внедрения нейросетей, связанные с безопасностью, возможной предвзятостью искусственного интеллекта и этикой, а также перспективы развития.**

**Ключевые слова:** нейронные сети, машинное обучение, искусственный интеллект, информационная безопасность, интеграция, закономерности

# NEURAL NETWORK PREDICTION OF INFORMATION SECURITY INCIDENTS

**Beliaeva T.A.[1] , Mikryukov A.A.[1]**

*[1] Plekhanov Russian University of Economics, Moscow,e-mail: tanbel03@mail.ru*

**Abstract**

**This work contains a description of the possibilities of using neural networks as an effective tool for ensuring information security. In the context of a rapidly changing cyber environment, the use of neural networks not only strengthens protection against new threats and attacks, but also creates a stable basis for the development of adaptive security strategies. The relevance of this study is due to the increasing prevalence of implementation of artificial intelligence technologies in various fields. The presented solution to the problems of incident forecasting using Python and the scikit-learn library allows you to increase the reliability of protection by preventing the emergence of a large number of new threats and attacks, which also allows you to evaluate the effectiveness of security measures, optimize resource allocation and plan security strategies. In addition, statistics provide a basis for training artificial intelligence systems in the field of cyber and information security, which contributes to more accurate forecasting and adaptation to changing threats, and also enables real-time analysis. This comprehensive approach provides organizations with the tools to optimize resource allocation, plan security strategies, and improve the effectiveness of their overall security posture. In addition, the work discusses potential problems in the implementation of neural networks related to security, possible bias of artificial intelligence and ethics, as well as development prospects**

**Keywords:** neural networks, machine learning, artificial intelligence, information security, integration, patterns

## *Введение*

В эпоху постоянного развития цифровой среды, угрозы в области кибербезопасности становятся все более сложными и распространенными. Это требует изменения подхода и внедрения новых методов в сферу защиты информации. Ожидается, что темпы роста

искусственного интеллекта (ИИ) в период с 2023 по 2030 составят 37 процентов в год [6], и в этом контексте искусственный интеллект, в частности нейронные сети, становятся важным элементом новой парадигмы в обеспечении безопасности в сети. Эти технологии не только меняют традиционные методы защиты, но и предоставляют организациям расширенные возможности в обнаружении угроз, распознавании образов и адаптивном обучении. В настоящее время способность нейронных сетей точно распознавать закономерности становится бесценным инструментом в стратегии противостояния киберпреступности.

Одним из ключевых преимуществ интеграции нейронных сетей в кибербезопасность является улучшение возможностей обнаружения угроз. Традиционные системы безопасности часто полагаются на подходы, основанные на правилах, которые могут с трудом успевать за быстро развивающимися тактиками, используемыми киберпреступниками. Нейронные сети, с другой стороны, превосходно выявляют сложные закономерности и аномалии в наборах данных, позволяя на ранней стадии обнаруживать потенциально вредоносные действия [4].

*Цель исследования*

Цель статьи заключается в исследовании и обосновании эффективности применения нейронных сетей для прогнозирования инцидентов в области информационной безопасности. В исследовании продемонстрировано, как использование нейросетей, основанных на языке программирования Python, может повысить надежность защиты, предупреждая новые угрозы, и способствовать более точному анализу и адаптации к изменяющимся сценариям кибербезопасности.

*Материал и методы исследования*

Известно, что нейронные сети являются хорошими функциональными аппроксиматорами, способными по таблично заданному временному ряду в результате обучения запомнить и восстановить вид функциональной зависимости этого ряда [1]. Это свойство легло в основу широкого применения нейронных сетей в системах поддержки принятия решений.

Эффективность нейросетевой аппроксимации сравнима с эффективностью нечеткой и нейро нечеткой аппроксимации экспериментальных данных. Способность нейронных сетей после обучения к обобщению и пролонгации результатов создает возможности и предпосылки для построения на их основе прогностических систем, которые способны обеспечивать возможность долгосрочного прогнозирования и обобщения данных в широком контексте систем поддержки принятия решений [3].

Так, одним из способов использования нейронных сетей в сфере информационной безопасности может стать прогнозирование количества инцидентов на основе статистики

инцидентов за последние несколько лет. Пусть дан временной ряд *x(t)* на промежутке *t*=1. Тогда задача прогнозирования состоит в том, чтобы найти продолжение временного ряда на неизвестном промежутке. Прогнозирующая нейронная сеть должна иметь один выход и количество входов, определяющее число учитываемых предыдущих значений ряда для прогнозирования, например, четыре последних значения. Для обучения нейронной сети необходимо подготовить обучающую выборку, в которой входными значениями будут количество инцидентов информационной безопасности предприятия за текущий период, а желаемым выходом – известное число инцидентов на следующий за ними год.

Метод ближайшего соседа (k-Nearest Neighbors, k-NN) (рис. 1) — один из самых простых и эффективных алгоритмов обучения с учителем, использующийся для классификации данных в нейронных сетях [2]. Он широко используется для поиска в доступном наборе данных, связывая новые точки данных с аналогичные существующими точками и является наиболее подходящим в контексте данного нейросетевого прогнозирования, так как он позволяет эффективно учитывать временные зависимости и тренды в данных.

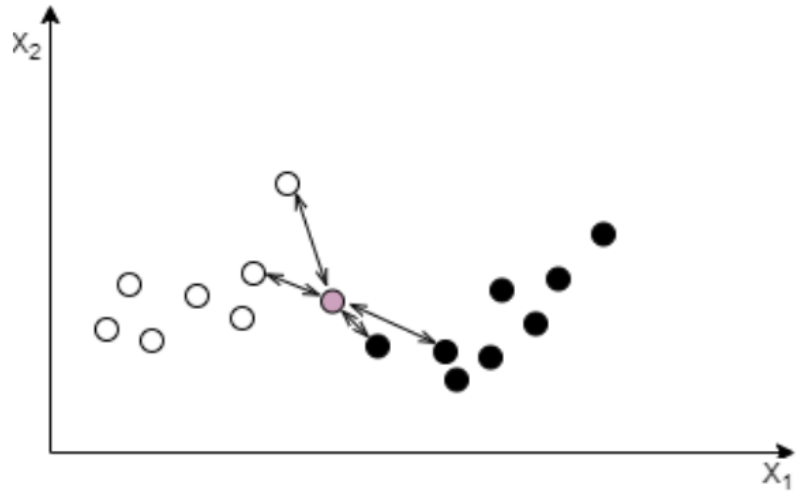


Рис.1 - Репрезентация метода ближайшего соседа

При использовании нейросетей в этом контексте, метод ближайшего соседа может быть применен к выходам нейросети. Например, для задачи временного ряда инцидентов, выходы нейросети для предыдущих временных точек могут быть использованы для поиска близких соседей в пространстве признаков и определения вероятности возникновения инцидента в следующий момент времени.

В этом методе для нового инцидента прогнозы строятся на основе близких, предшествующих инцидентов в пространстве признаков. Это означает, что инциденты, которые имеют схожие характеристики, будут использоваться для определения вероятности и характера будущих инцидентов. Этот метод основан на принципе анализа похожести, что особенно важно в предсказании инцидентов, где паттерны могут быть схожими с предыдущими периодами.

Этот подход позволяет комбинировать преимущества нейросетевого моделирования и метода ближайшего соседа для более точного и адаптивного прогнозирования инцидентов в области информационной безопасности.

*Результаты исследования и их обсуждение*

В ходе исследования и обучения нейросети с помощью языка программирования Python и python-библиотеки для машинного обучения scikit-learn было инициализировано оптимальное число k- ближайших соседей. Результаты влияния выбранного для обучения количества соседей на точность прогноза представлены на рисунке 2. В ситуации с четырьмя столбцами входных данных, самым эффективным является обучение с 3 соседями.

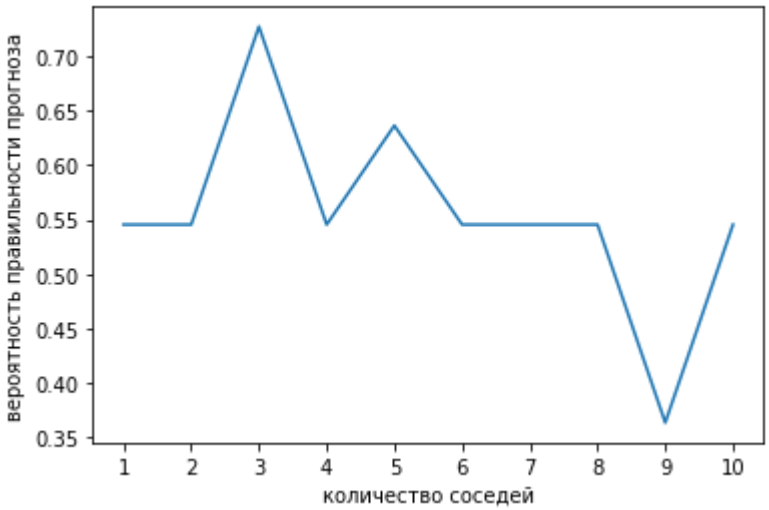


Рис.2 - График нахождения оптимального числа соседей для обучения модели

Входные данные для обучения модели представлены на рисунке 3.

| Вх0 | Вх1 | Вх2 | Вх3 | Вых. |
|---|---|---|---|---|
| 1342 | 1241 | 1186 | 1444 | 1285 |
| 1241 | 1186 | 1444 | 1285 | 1169 |
| 1186 | 1444 | 1285 | 1169 | 1025 |
| 1444 | 1285 | 1169 | 1025 | 1138 |
| 1285 | 1169 | 1025 | 1138 | 1494 |
| 1169 | 1025 | 1138 | 1494 | 1116 |
| 1025 | 1138 | 1494 | 1116 | 1289 |
| 1138 | 1494 | 1116 | 1289 | 1380 |
| 1494 | 1116 | 1289 | 1380 | 1005 |
| 1116 | 1289 | 1380 | 1005 | 1394 |
| 1289 | 1380 | 1005 | 1394 | 1238 |
| 1380 | 1005 | 1394 | 1238 | 1219 |
| 1005 | 1394 | 1238 | 1219 | 1246 |
| 1394 | 1238 | 1219 | 1246 | 1482 |
| 1238 | 1219 | 1246 | 1482 | 1322 |

...

Рис.3 - Входные и выходные данные модели

Используя метод k-NN, модель анализирует ближайших соседей для каждого значения входных данных, определяя их влияние на прогноз для следующего года. Модель обучается на тренировочных данных, а затем оценивается на тестовых данных для проверки ее производительности и точности прогнозирования. В итоге, обученная модель, получая на вход 4 значения количества инцидентов за предыдущий период выдаст предсказание о количестве инцидентов на следующий год.

Прогнозирование количества инцидентов информационной безопасности на основе статистики предыдущих лет обеспечивает организациям предупреждение о возможных угрозах и позволяет преждевременно готовиться к предстоящим вызовам. Это также позволяет оценивать эффективность мер безопасности, оптимизировать распределение ресурсов и планировать стратегии безопасности [7]. Кроме того, статистика предоставляет базу для обучения систем искусственного интеллекта в области кибербезопасности, что способствует более точному прогнозированию и адаптации к изменяющимся угрозам.

Также нейронные сети могут применяться в информационной и кибер безопасности со стороны других перспектив. Например, нейронные сети могут быть использованы для проведения поведенческий анализа для установления базовой линии нормальной деятельности пользователя и системы. Постоянно обучаясь и адаптируясь к изменениям, они могут выявлять аномалии, которые при дальнейшем анализе укажут на угрозы безопасности. Этот подход в кибербезопасности особенно эффективен при обнаружении ранее неизвестных атак или атак нулевого дня [5].

Помимо этого, нейронные сети справляются с распознаванием образов, что делает их идеальными для анализа больших объемов данных сетевого трафика. Благодаря контролируемому обучению нейронные сети можно обучить на помеченных наборах данных, чтобы различать нормальное и вредоносное поведение сети. Они анализируют сетевой трафик, журналы и поведение пользователей для выявления аномалий и угроз, автоматизируют реагирование и улучшают свою производительность с течением времени, обучаясь на обратной связи [9]. В результате они повышают точность и эффективность анализа трафика, обеспечивая более надежную защиту от развивающихся киберугроз.

*Проблемы и будущие перспективы:*

В ходе исследования были выявлены следующие преимущества использования нейронных сетей в системах информационной безопасности:

- Адаптивность: Системы кибербезопасности на базе нейронных сетей постоянно адаптируются, учась на предыдущих атаках, что затрудняет повторное использование уязвимостей злоумышленниками.

- Точность: способность различать тонкие закономерности приводит к более точной классификации, уменьшая количество ложно положительных и отрицательных результатов.
- Анализ в реальном времени: позволяет быстро выявлять инциденты безопасности и реагировать на них.
- Снижение количества человеческих ошибок: автоматизированная классификация снижает зависимость от ручного анализа, сводя к минимуму риск человеческой ошибки.

Хотя интеграция нейронных сетей в кибербезопасность имеет огромные перспективы, она не лишена проблем. Обеспечение этичного использования ИИ, решение проблем, связанных с предвзятостью в обучающих данных, создание надежных мер безопасности для защиты самих нейронных сетей, а также непрерывный мониторинг и обновление для поддержания эффективности против развивающихся угроз — важные факторы для организаций, которые готовы решиться применять нейронные сети при разработке и обеспечении информационной политики [8].

Помимо этого, обеспечение конфиденциальности в моделях искусственного интеллекта имеет критическое значение, сопоставимое с важностью кибербезопасности. Модели ИИ, случайно раскрывающие личную информацию в процессе анализа угроз, могут сделать системы уязвимыми для будущих неожиданных атак. Ключевая задача заключается в том, чтобы обучить модели ИИ эффективно справляться с различными кибератаками, при этом оптимизируя время реагирования и сохранение конфиденциальности.

Однако надежные наборы данных для обучения с учетом конфиденциальности являются редкостью, так как организации не готовы обмениваться данными, содержащими персональную или конфиденциальную информацию. Для решения этой проблемы применяются методы генеративного моделирования, такие как генеративно-состязательные сети (Generative adversarial network, GAN), которые создают суррогатные модели данных, обеспечивая сохранение конфиденциальности при сохранении их полезности для обучения.

Одним из наиболее безопасных решений в данной ситуации является двойной подход, использующий модели глубокого обучения, сохраняющие конфиденциальность, и сочетающий генеративное моделирование с символическими графами знаний (Knowledge Graph, KG), выражающими предметные знания [8]. Этот подход повышает сохранение конфиденциальности в генерируемых данных для последующих задач машинного обучения.

*Заключение*

Использование нейронных сетей в кибербезопасности представляет собой крупный шаг вперед, который позволит организациям повысить уровень безопасности в условиях растущего количества утечек данных и атак. Представленный подход к нейросетевосму

прогнозированию инцидентов с помощью языка программирования Python обеспечивает сбалансированный и комплексный механизм предсказания инцидентов, способствующий укреплению общей кибербезопасности и эффективному реагированию на динамичные сценарии кибератак. Эксперты по кибербезопасности, применяя нейронные сети, могут эффективнее выявлять угрозы, проводить поведенческий анализ и оперативно реагировать на изменения в безопасности.

**Список литературы**


1. Аппроксимация функций с помощью нейронных сетей и нечетких систем// Журнал “Проблемы управления” [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/approksimatsiya-funktsiy-s-pomoschyu-neyronnyh-setey-i-nechetkih-sistem (дата обращения 18.12.2023)
2. Гудфеллоу Я., Бенджио И., Курвилль А. − Глубокое обучение, 2017 г. с.106-110
3. Микрюков А.А., Бабаш А.В., Сизов В.А. Классификация событий в системах обеспечения информационной безопасности на основе нейросетевых технологий. Открытое образование. 2019. Т.23. №1. С. 57-63.
4. Микрюков А.А., Усцелемов В.Н. Гибридная модель оценки рисков в информационных системах. Прикладная информатика. 2014. №1. (49) С 50-55.
5. Aritran Piplai , Anantaa Kotal, Seyedreza Mohseni, Manas Gaur , Sudip Mittal, and Anupam Joshi, Knowledge-enhanced Neuro-Symbolic AI for Cybersecurity and Privacy, Bibtex, 2023, P. 1-2
6. Deep learning - statistics & facts// Statista [Электронный ресурс]. URL: https://www.statista.com/topics/9586/deep-learning/#topFacts (дата обращения 17.12.2023)
7. Intrusion Detection with Neural Networks// Advances in Neural Information Processing Systems 10 (NIPS 1997) [Электронный ресурс]. URL: https://proceedings.neurips.cc/paper_files/paper/1997/hash/1abb1e1ea5f481b589da52303b091cbb-Abstract.html (дата обращения 18.12.2023)
8. Marek Pawlicki, Rafał Kozik, Michał Choraś,A survey on neural networks for (cyber-) security and (cyber-) security of neural networks, Neurocomputing, Volume 500, 21 August 2022, Pages 1075-1087
9. THE APPLICATION OF NEURAL NETWORK FOR CYBERSECURITY// Форум молодых ученых [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/the-application-of-neural-network-for-cybersecurity (дата обращения 19.12.2023)