

Научный руководитель:

Байрушин Ф.Т.

Уфимский университет науки и технологий, Уфа

## **ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ**

**Аннотация.** В данной статье рассматривается применение нейросетевых технологий в сфере нейронных сетей для повышения уровня информационной безопасности предприятий. Выражается необходимость внедрения новых методов анализа сетевого трафика, выявления ошибок и угроз предприятию. Рассматриваются эффективность, достоинства и недостатки нейросетей для при внедрении нейросетей в организацию работы предприятия, даются примеры компаний внедривших нейросети в компании для повышения уровня безопасности.

**Ключевые слова:** безопасность, кибератака, защита, угроза, нейросеть.

Информационная безопасность является одним из важнейших аспектов деятельности любого современного предприятия, особенно в условиях

стремительного роста числа кибератак и иных угроз. Старые способы защиты без использования продвинутого искусственного интеллекта – антивирусы, которые к сожалению, уже не такие эффективные. Именно здесь на помощь приходят технологии искусственного интеллекта и нейросети, способные анализировать огромные объемы данных и выявлять потенциальные угрозы в режиме реального времени.

Нейросети являются хорошим механизмом для защиты предприятий и иных организаций. Преимущества нейросетевых технологий таковы:

1. Автоматизация. Внедрив в нейросеть способность распознавать и ликвидировать угрозы без постоянного присутствия человека позволит, таким образом, распределить трудовые ресурсы по другим направлениям. Это позволит компаниям грамотно реорганизовывать рабочий процесс, добиваясь большей эффективности, что в свою очередь двигает компанию вперед.

2. Адаптация защиты. Одна из крайне положительных способностей нейросетей – это самообучение. Благодаря самообучению, нейросеть может приспосабливаться на опыте защиты ПО к новым технологическим ухищрениям хакеров и их вирусам, способных выкрасть, испортить или исказить информацию поступающую из предприятия в предприятие и внутри предприятия. Это позволит сделать защиту гибкой без необходимости своевременно писать коды для защиты ПО, с этим справится машина самостоятельно, главное лишь следить, чтобы она это делала правильно.

3. BigData или масштабируемость. В условиях цифрового общества своевременная и правильно структурированная информация делается необходимостью. Развитие нейросетей дала возможность сделать нейросети более продвинутыми, внедрив в них технологию BigData, что позволило компаниям, обладающим огромным размером информационной структуры, быстро обрабатывать огромные потоки информации, позволяя принимать правильные и своевременные решения. Технология нейросетей имеет довольно большой спектр возможного применения в сфере защиты информации. Например, распознавание лиц. Нейросеть запоминает лица сотрудников производства, что позволяет защищать аппаратуру и иное имущество компании от чужаков.

4. Cafee – пространство для точного обучения, является опенсорсом. Выполняет упорядочивание картинок и иных изображений с использованием нейросетей.

5. Анализ поведения пользователей и сотрудников. Каждая компания желает сохранить свое существование на рынке. И чтобы сохранить себя на рынке она будет отслеживать поведение пользователей и сотрудников. Нейросети, участвуя в этом процессе, позволяют максимизировать полезность в данной сфере. Через голос и биометрию нейросеть может обнаружить чужака в компании, посланного для шпионажа, диверсии и прочих пакостей.

6. Мониторинг сетевого трафика. Мониторинг сетевого трафика является крайне важным процессом в отношении защиты информационной безопасности. Нейросети необходимо провести анализ информации, идущей через адаптеры WIFI роутеры и прочие способы передачи информации для обнаружения в ней вредоносной для компаний информации.

7. Управление идентификацией и аутентификацией. Биометрия является сейчас довольно популярной технологией для защиты общественных мест. Например, аэропорта как место сосредоточения пассажиров. Вся биометрия (отпечатки пальцев, глаза, голос), которую можно проверить на отличительные свойства, используется для проведения и идентификации и аутентификации личности сугубо в защитных интересах. Но, несмотря на наличие бесспорных плюсов, нейросети обладает рядом недостатков и издержек.

Издержки и недостатки:

1. Отсутствие квалифицированных специалистов: для предприятий и, в особенности для России, насущна проблема нехватки программистов, способных обеспечивать качественную работу нейронных сетей. Проблема нехватки кадров не позволяет популяризовать использование нейросетей в России ровно до тех пор, пока не будет доступного количества специалистов.

2. Необходимость большого объема качественных данных и добросовестного ведения отчетности: для эффективной работы необходим большой набор данных, которые нейросеть сможет обрабатывать, и учится, совершенствуя свои навыки. Небольшие компании не смогут предоставить достаточного количества данных для качественного приспособления нейросети под специфику работы своей компании, что приведет к некачественной работе нейросети.

3. Высокая стоимость внедрения: малая доступность также обуславливается высокой стоимостью работы нейросети. На данный момент технология не является доступной и требует большого количества высококвалифицированных специалистов, что, следовательно, затребует большое количество финансов на оплату услуг таких специалистов. У небольших компаний таких денег нет и им приходится работать по-старому, или полагаться на специалистов качеством ниже.

4. Уязвимость самих нейросетей: несмотря на продвинутость технологии, де-факто дарующая бесконечно оптимистичные перспективы на данный момент нейросети не идеальны. Уязвимость заключается в качестве даваемых ему на обработку данных. Неправильная, то есть ошибочная информация, крайне вредоносна в перспективе для обучения нейросети, которая может делать неправильные выводы, что будет приводить к статистическим ошибкам и потерям компаний.

Разобрав все достоинства и недостатки, следует рассмотреть примеры использование нейросетей: авангардом использования нейросетей выступают передовые компании мира: Google, использующие машинное

обучение и нейронные сети для повышения безопасности, Microsoft в рамках Microsoft 365 и Azure используют машинное обучение для анализа поведенческих паттернов пользователей и обнаружения потенциально опасных действий и IBM использует нейронные сети и другие методы машинного обучения для защиты данных и документооборота.

Нейросети являются очень важной составляющей современной информационной безопасности. Их использование и внедрение во все большее количество предприятий является важной с точки зрения и практической, и теоретической. Технология расширяет возможности обеспечения информационной безопасности. Нейросети за годы существования были достаточно доработаны, чтобы повысить уровень защищенности архитектуры ПО и минимизировать риски вреда для ПО. Успех работы нейросети зависит от профессионализма сотрудников. Исследования в области нейросетей должны быть направлены на увеличение защищенности к внешним воздействиям, самостоятельности в сфере обучения и совершенствования BigData.

#### **Список использованных источников:**

1. Резник Д.В. Искусственные нейросети. Анализ возможностей использования в целях обеспечения информационной безопасности // The Scientific Heritage 2021. С. 50–51. URL: <https://cyberleninka.ru/article/n/iskusstvennye-neyroseti-analiz-vozmozhnostey-ispolzovaniya-v-tselyah-obespecheniya-informatsionnoy-bezopasnosti>.
2. Прохоров А.С. Применение нейронных сетей для обеспечения безопасности человека в жилых и промышленных помещениях // Символ науки. 2021. С. 25–29. URL: <https://cyberleninka.ru/article/n/primenie-neyronnyh-setey-dlya-obespecheniya-bezopasnosti-cheloveka-v-zhilyh-i-promyshlennyh-pomescheniyah>.
3. Тихолаз Р.В. Обеспечение информационной безопасности документооборота с использованием нейронных сетей // Документ в современном обществе. 2024. С. 584–586. URL: [https://elar.urfu.ru/bitstream/10995/140754/1/978-5-7996-3940-2\\_2024\\_135.pdf](https://elar.urfu.ru/bitstream/10995/140754/1/978-5-7996-3940-2_2024_135.pdf).

**Akhmadullin R.A.**  
Ufa University of Science and Technology, Ufa

Scientific supervisor:  
**Bayrushin F.T.**  
Ufa University of Science and Technology, Ufa

## **USING NEURAL NETWORKS TO ENSURE INFORMATION SECURITY AT THE ENTERPRISE**

**Abstract.** This article discusses the application of neural network technologies in the field of neural networks to enhance the information security of enterprises. It emphasizes the need to implement new methods for analyzing network traffic, detecting errors and threats within organizations. The effectiveness, advantages, and disadvantages of neural networks for enterprise integration are examined, along with examples of companies that have implemented neural networks to improve security levels.

**Keywords:** security, cyberattack, protection, threat, neural network.