Егоркин Александр Александрович, студент,
Калужский филиал МГТУ им. Н.Э. Баумана,
г. Калуга

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: Исследование и применение ИНС в области ИБ находятся на стыке передовых технологий и комплексных методов защиты. Нейронные сети обладают способностью к обучению на основе обширных объемов данных, что позволяет им адаптироваться к новым сценариям угроз. Они могут быть применены для выявления аномалий, анализа трафика, оценки поведения пользователя, фильтрации спама и вредоносных программ.

Ключевые слова: искусственные нейронные сети, информационная безопасность, угрозы, методы защиты информации.

Искусственные нейронные сети (ИНС) нашли широкое и разнообразное применение в области информационной безопасности благодаря своей способности адаптироваться, обучаться на больших объемах данных и выявлять сложные паттерны и аномалии. Они применяются в нескольких ключевых аспектах обеспечения кибербезопасности:

1. *Обнаружение угроз и аномалий:* ИНС применяются для непрерывного анализа больших объемов данных с целью выявления необычных или вредоносных активностей. Это позволяет оперативно реагировать на потенциальные угрозы.
2. *Анализ сетевого трафика:* искусственные нейронные сети способны обнаруживать аномальный сетевой трафик, что помогает идентифицировать подозрительную активность, включая атаки типа DDoS (распределенный отказ от обслуживания) или подозрительные попытки несанкционированного доступа.
3. *Идентификация аномалий в поведении пользователей:* нейронные сети используются для анализа поведения пользователей и выявления аномальных активностей, указывающих на возможные угрозы. Это позволяет выявить необычные запросы, несанкционированный доступ или другие подозрительные действия.
4. *Фильтрация спама и вредоносных программ:* нейронные сети могут быть обучены распознавать паттерны спама, фишинга или вирусов, что помогает в создании эффективных систем фильтрации.
5. *Улучшение систем безопасности IoT:* для защиты интернета вещей от кибератак, ИНС могут использоваться для обнаружения аномалий в сетях IoT и защиты устройств [1].

Но, несмотря на это, использование искусственных нейронных сетей в области информационной безопасности вызывает определенные затруднения, которые важно учитывать:

1. **Необходимость большого объема данных:** для эффективного обучения ИНС требуется большое количество данных. В случае информационной безопасности, особенно в обнаружении новых угроз, может быть недостаточно данных для корректного и полного обучения нейронных сетей.
2. **Сложность в обработке разнородных данных:** В области информационной безопасности данные часто разнообразны по типу, формату и источнику. Обработка и анализ таких данных требует сложных моделей ИНС и специализированных подходов к их использованию.

3. **Объяснимость и интерпретируемость:** иногда ИНС работают как "черный ящик", их принятие решений может быть сложно объяснить. В области безопасности требуется возможность объяснения и интерпретации принятых решений для выявления причин угроз и аномалий.
4. **Уязвимость к атакам:** сами ИНС могут быть подвержены атакам. Атаки вроде атак на обучение (adversarial attacks) могут обмануть ИНС, приводя к неправильным или вредоносным выводам.
5. **Требования к вычислительным ресурсам:** обучение и эксплуатация сложных нейронных сетей требуют больших вычислительных мощностей и инфраструктуры, что может быть затратным с точки зрения времени и ресурсов.
6. **Конфиденциальность данных:** использование ИНС часто требует доступа к конфиденциальным данным для обучения. Это может создавать риски конфиденциальности, особенно при работе с информацией под грифом секретности.
7. **Интеграция с существующими системами:** иногда интеграция ИНС с существующими системами информационной безопасности может быть сложной из-за различий в архитектуре и подходах.
8. **Тестирование и верификация:** Тестирование и верификация ИНС являются сложными задачами, особенно при необходимости демонстрации их эффективности и надежности перед внедрением в реальные условия.
9. **Отсутствие контроля за результатами:** искусственные нейронные сети могут быть сложными в управлении и контроле за результатами. Иногда их поведение может быть неожиданным или непредсказуемым, что усложняет их управление и поддержку.
10. **Возможность ошибок и ложных срабатываний:** Даже при высокой точности ИНС существует вероятность ложных срабатываний или ошибок в определении угрозы. Это может привести к проблемам с доверием к системе и необходимости дополнительной верификации результатов.
11. **Эволюция угроз и технологий:** с течением времени угрозы в области информационной безопасности постоянно развиваются, а технологии ИНС также требуют обновлений и улучшений для эффективного противодействия новым видам атак.
12. **Поддержка и обслуживание:** обслуживание и поддержка ИНС может также потребовать специализированных знаний и опыта, что может создать дополнительные сложности при их использовании в области информационной безопасности.
13. **Этические вопросы:** важно учитывать этические аспекты использования ИНС в сфере безопасности, такие как использование личных данных, принятие решений на основе данных и другие нюансы [2, 3].

Учитывая эти проблемы, внедрение ИНС в сферу информационной безопасности требует осторожного подхода и учета рисков и ограничений, чтобы максимально эффективно использовать их преимущества. Эти проблемы не исключают применения ИНС в информационной безопасности, но подчеркивают важность комплексного и обдуманного подхода при их использовании, а также необходимость развития инновационных методов для преодоления этих проблем.

В целом, искусственные нейронные сети представляют собой мощный инструмент в борьбе с угрозами информационной безопасности, но их применение требует тщательного анализа и учета рисков. Дальнейшие исследования и разработки в этой области могут помочь улучшить надежность и эффективность применения нейронных сетей в защите информации, учитывая и минимизируя выявленные ограничения.

Список литературы:

1. Марков Г.А. Использование технологий нейронных сетей при решении задач информационной безопасности // Молодежный научно-технический вестник. –2014. – № 3.

2. Ридкокаша А.А., Голдер К.К. Основы систем искусственного интеллекта. Учебное пособие. Черкассы: Эхо-Плюс, 2002. – 240с.

3. Хамит, Адильхан Усипалиулы. Использование искусственных нейронных сетей для решения задач информационной безопасности / Адильхан Усипалиулы Хамит. // Молодой ученый. – 2023. – № 36.