УДК 004

МАШИННОЕ ОБУЧЕНИЕ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Антонов А.С., старший оператор научной роты, I курс
Военная академия связи имени Маршала Советского Союза С.М. Будённого, г. Санкт-Петербург

Машинное обучение (МО) становится неотъемлемой частью стратегий обеспечения информационной безопасности (рисунок 1) [1-4], играя важную роль в выявлении и предотвращении киберугроз [5]. В этой статье рассмотрим, как МО находит применение в защите информации от потенциальных угроз.

Рисунок 1 – Машинное обучение в информационной безопасности

Одной из ключевых областей применения машинного обучения является обнаружение аномалий. Алгоритмы машинного обучения способны анализировать объемные наборы данных и выявлять отклонения от нормы [6, 7]. Это позволяет быстро обнаруживать подозрительную активность, которая может указывать на попытку несанкционированного доступа или другие виды атак.

Технологии машинного обучения также активно применяются в системах детекции вторжений [8]. Способность алгоритмов адаптироваться к изменяющимся сценариям атак делает их эффективными в выявлении новых угроз, неизвестных традиционным методам [9]. Это создает более устойчивую линию обороны в условиях постоянно меняющейся киберугрозовой среды.

Прогнозирование потенциальных угроз – еще один аспект, в котором машинное обучение проявляет свою силу [10]. Анализ данных и паттернов помогает выявить возможные слабые места в системах безопасности и принять меры по их усилению еще до возникновения рисков.

Системы машинного обучения также играют ключевую роль в улучшении систем аутентификации и управлении доступом [11]. Биометрическое распознавание, анализ поведения пользователей и другие методы, основанные на МО, повышают уровень безопасности при входе в систему, минимизируя риски несанкционированного доступа.

Однако, несмотря на все преимущества, внедрение машинного обучения в области информационной безопасности также предъявляет вызовы. Обучение алгоритмов требует большого объема данных, а также постоянного мониторинга и обновления систем для поддержания их эффективности.

В заключение, машинное обучение становится надежным союзником в борьбе с киберугрозами, обеспечивая более интеллектуальные и гибкие методы защиты информации. Постоянное развитие этих технологий содействует созданию более устойчивых и безопасных цифровых сред.

Список литературы:

1. Методы восстановления непараметрической регрессии в условиях несбалансированных данных / А. Д. Салычева и др. – Вологда : Общество с ограниченной ответственностью "Издательство "Инфра-Инженерия", 2024. – 192 с. – ISBN 978-5-9729-1856-0. – EDN AAJATW.
2. Свидетельство о государственной регистрации программы для ЭВМ № 2023684619 Российская Федерация. Efficient Network: № 2023684038: заявл. 14.11.2023: опубл. 16.11.2023 / П. А. Пылов.
3. Свидетельство о государственной регистрации программы для ЭВМ № 2023680070 Российская Федерация. Модернизированная модель DBSCAN для определения скрытых взаимосвязей : № 2023668841 : заявл. 13.09.2023 : опубл. 26.09.2023 / Р. В. Майтак. – EDN KQUUKF.
4. Асимптотический анализ поведения прикладных моделей машинного обучения : Учебное пособие / А. В. Протодьяконов и др. – Вологда : Общество с ограниченной ответственностью "Издательство "Инфра-Инженерия", 2023. – 144 с. – ISBN 978-5-9729-1455-5. – EDN APHQME.
5. Свидетельство о государственной регистрации программы для ЭВМ № 2023680124 Российская Федерация. BrainPower : № 2023669010 : заявл. 16.09.2023 : опубл. 26.09.2023 / Р. В. Майтак. – EDN QXBJIM.
6. Математические и программные методы построения моделей глубокого обучения : Учебное пособие / А. В. Протодьяконов и др. – Вологда : Общество с ограниченной ответственностью "Издательство

"Инфра-Инженерия", 2023. – 176 с. – ISBN 978-5-9729-1484-5. – EDN PZLUAH.

7. Свидетельство о государственной регистрации программы для ЭВМ № 2023680335 Российская Федерация. Maitak Intelligence Natural Language Processing Module : № 2023669704 : заявл. 27.09.2023 : опубл. 28.09.2023 / Р. В. Майтак.
8. Свидетельство о государственной регистрации программы для ЭВМ № 2023684621 Российская Федерация. Destructed Deep Random Forest: № 2023684050: заявл. 14.11.2023: опубл. 16.11.2023 / П. А. Пылов.
9. Свидетельство о государственной регистрации программы для ЭВМ № 2023684622 Российская Федерация. Mask Made AI: № 2023684042: заявл. 14.11.2023: опубл. 16.11.2023 / П. А. Пылов.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2023680103 Российская Федерация. Cognitive Solution : № 2023669189 : заявл. 19.09.2023 : опубл. 26.09.2023 / Р. В. Майтак. – EDN QEMFJA.
11. Свидетельство о государственной регистрации программы для ЭВМ № 2023684624 Российская Федерация. Программа автоматического распознавания лиц в видеопотоке: № 2023684236: заявл. 15.11.2023: опубл. 16.11.2023 / П. А. Пылов.