УДК 316.6

ТЮЛЬПАНОВ А. И., студент учебной группы 3272
Военная академия связи имени С.М. Будённого
г. Санкт-Петербург

ЗАЩИТА ИНФОРМАЦИИ В ЦИФРОВУЮ ЭПОХУ С ПОМОЩЬЮ ТЕХНОЛОГИЙ ИИ

В результате развития технологий и появления искусственного интеллекта (ИИ) в современном мире все мы сталкиваемся с новыми вызовами в области защиты информации. Искусственный интеллект предоставляет огромные возможности для улучшения нашей жизни и бизнеса, но в то же время он создает новые уязвимости и риски для безопасности данных [1, 2].

Одним из основных аспектов, требующих внимания в области защиты информации, является возможное использование ИИ для кибератак (см. рисунок 1). Киберпреступники могут использовать алгоритмы машинного обучения и нейронные сети для создания более сложных и неотслеживаемых атак на информационные системы. Это означает, что традиционные методы обнаружения и предотвращения киберугроз могут быть недостаточно эффективными, вследствие чего необходимо разработать новые методы защиты [3].

Рисунок 1. Схема нападения на информационные системы с помощью ИИ-кибератак

Еще одним важным аспектом является проблема конфиденциальности информации. С ростом количества данных, собираемых и обрабатываемых системами ИИ, возникает и необходимость в более строгих механизмах защиты приватности пользователей [4]. Компании и организации должны быть бдительными в отношении сбора и хранения персональной информации, а также в обеспечении её защиты от несанкционированного доступа.

Борьба с фейковыми новостями и манипуляциями тоже становится важным аспектом защиты информации в эпоху ИИ. Алгоритмы машинного обучения могут использоваться для создания и распространения дезинформации, что представляет угрозу для общественного спокойствия и политической стабильности. С целью борьбы с этим явлением необходимо развивать технологии обнаружения и фильтрации поддельных новостей [5], а также повышать информационную грамотность среди пользователей.

Тем не менее, при всём этом важно учитывать этические аспекты использования ИИ в области защиты информации. Вопросы приватности, справедливости и прозрачности должны быть в центре внимания при разработке и внедрении новых технологий. Необходимо обеспечивать баланс между использованием ИИ для защиты данных и защитой прав и свобод пользователей [6].

В целом, современная эпоха искусственного интеллекта представляет как новые возможности, так и новые вызовы в области защиты информации. Развитие технологий и совершенствование методов защиты являются ключевыми компонентами обеспечения безопасности данных в быстро меняющемся цифровом мире. Одним из перспективных направлений в области защиты информации в эпоху искусственного интеллекта является использование самого ИИ для усиления кибербезопасности. Технологии машинного обучения и анализа больших данных могут быть применены для обнаружения аномалий в сетевом трафике, выявления несанкционированных действий пользователей и автоматизации процессов реагирования на киберугрозы [7]. Это позволяет сократить время реакции на инциденты безопасности и повысить эффективность защитных мер.

Еще одним важным аспектом в этом плане является развитие квантовой криптографии, которая предлагает новые методы шифрования данных, устойчивые к атакам квантовых компьютеров. Переход к квантово-стойким шифрам может обеспечить более высокий уровень защиты данных в условиях развития квантовых технологий [8].

Кроме всего прочего, и самим людям в составе правительств и корпораций важно активно сотрудничать на международном уровне для борьбы с киберугрозами. Обмен информацией о новых угрозах и совместные усилия в области кибербезопасности могут помочь эффективнее противодействовать киберпреступности и защищать критически важную информацию.

Наконец, обучение и осведомленность пользователей, в сущности, играют ключевую роль в обеспечении безопасности данных в современном мире. Регулярная реализация обучающих программ по кибербезопасности, а также повышение информационной грамотности, — вот меры, которые помогут снизить риск успешных кибератак и защитить личные данные.

В заключение можно сказать, что защита информации в современную эпоху искусственного интеллекта представляет собой сложную и многогранную задачу, требующую комплексного подхода и постоянного развития. Только совместными усилиями государств, компаний и общества в целом мы сможем обеспечить надежную защиту данных и тем самым обеспечить безопасное цифровое будущее.

Список литературы:

1. *Томас Кормен, Чарльз Лейзерсон.* Алгоритмы: построение и анализ, 3-е издание – М.: ООО И.Д. Вильямс. 2013. – 1328 с.
2. Свидетельство о государственной регистрации программы для ЭВМ № 2024611038 Российская Федерация. Sliding Window Predictor LLM : № 2023689243 : заявл. 25.12.2023 : опубл. 17.01.2024 / П. А. Пылов. – EDN AGNEAO.
3. Свидетельство о государственной регистрации программы для ЭВМ № 2023669862 Российская Федерация. Insight IQ : № 2023669164 : заявл. 19.09.2023 : опубл. 21.09.2023 / Р. В. Майтак. – EDN YCLTHP.
4. L. Graesser, W. L. Keng. Foundations of Deep Reinforcement Learning: Theory and Practice in Python. Addison-Wesley Professional, 2019.
5. Свидетельство о государственной регистрации программы для ЭВМ № 2024611019 Российская Федерация. Multi-view generation of 3D objects based on diffusion model : № 2024610024 : заявл. 02.01.2024 : опубл. 17.01.2024 / П. А. Пылов. – EDN CQQJRO.
6. 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.
7. Свидетельство о государственной регистрации программы для ЭВМ № 2024610491 Российская Федерация. Modified Switch Transformer : № 2023689285 : заявл. 25.12.2023 : опубл. 11.01.2024 / П. А. Пылов. – EDN LYISWR.
8. I. Isaev, S. Dolenko. Group Determination of Parameters and Training with Noise Addition: Joint Application to Improve the Resilience of the Neural Network Solution of a Model Inverse Problem to Noise in Data. Advances in Intelligent Systems and Computing, 2019, V.848, pp. 138-144. Springer, Cham. DOI: 10.1007/978-3-319-99316-4_18 (дата обращения: 21.08.2023).