УДК 004.056:004.8

Д. В. Мерзляков[1]

Российский государственный профессионально-педагогический университет

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ РЕШЕНИЯ ПОВСЕДНЕВНЫХ ЗАДАЧ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В работе рассматриваются основные принципы работы искусственного интеллекта, его возможности. Также описываются конкретные примеры использования искусственного интеллекта для обнаружения угроз, анализа безопасности данных. Рассматривается несколько алгоритмов, которые в наше время помогают сохранить персональные данные, также важные документы.

Ключевые слова: искусственный интеллект, нейронная сеть, машинное обучение, информационная безопасность.

В современном мире, где информация играет ключевую роль, электронный документооборот имеет неотъемлемую часть работы предприятий и организаций. Однако вместе с этим возрастает риск потери части документов или попадания каких-либо документов в руки злоумышленников, которые могут использовать их в своих целях. Поэтому компании начинают использовать искусственный интеллект для повышения эффективности защиты информации [Автоматизированная платформа безопасности].

Целью работы является применение информационной безопасности на основе искусственного интеллекта.

Информационная безопасность (ИБ) является совокупностью методов, технологий и процессов, направленных на защиту информации от несанкционированного доступа, изменения, уничтожения или утраты. Структура ИБ включает в себя следующие составляющие:

Физическая безопасность: защита информации от несанкционированного доступа к физическим носителям информации, таким как компьютеры, серверы, сетевые устройства и т.д.

Сетевая безопасность: защита информации от несанкционированного доступа через компьютерные сети, включая защиту от вирусов, троянских коней, спама и других видов сетевой угрозы.

Информационная безопасность: защита информации от несанкционированного доступа, изменения, уничтожения или утраты.

[1] Научный руководитель: С. В. Ляхов, кандидат технических наук, доцент, заведующий кафедрой РГППУ.

Прикладная безопасность: защита информации от несанкционированного доступа через прикладные программы, такие как веб-браузеры, электронные почты и т.д.

Управление информационной безопасностью: процессы, которые обеспечивают контроль и управление информационной безопасностью, включая политику, процедуры, инструкции и т.д.

В рамках корпоративной и производственной деятельности, документооборот является важным аспектом информационной безопасности. Документооборот включает в себя создание, хранение, обработку и уничтожение документов, которые содержат информацию. В этом контексте, информационная безопасность должна обеспечивать защиту документов от несанкционированного доступа, изменения, уничтожения или утраты.

В целом, информационная безопасность является важным аспектом деятельности любой организации, и ее структура и составляющие должны быть тщательно разработаны и реализованы, чтобы обеспечить защиту информации от различных угроз.

Именно при обработке большого объема данных результаты работы нейросетей не сопоставимы с другими технологиями и человеком. Модели способны не только применять статичный набор правил, но и постоянно самообучаться и совершенствоваться. По оценкам VK, нейросети и машинное обучение максимально эффективны в решениях по распознаванию и блокировке фишинга, фрода, спама, обнаружению ботов и детектированию сложных атак. За счет автоматизации реагирования на инциденты ИБ сокращается время реакции аналитиков и операторов на атаку и снижаются риски человеческой ошибки. С помощью машинного обучения можно значительно сократить количество ложных срабатываний, чтобы фокусироваться на реальных угрозах [Инфобезопасность].

ИИ и ML позволяют находить необычные поведения и паттерны, которые могут указывать на киберугрозы, обрабатывать большие объемы данных для выявления трендов и предсказания угроз, использоваться для автоматического обнаружения и блокировки вредоносного трафика, автоматизации поиска и устранения уязвимостей в системах.

Вот несколько примеров, как AI и ML могут быть использованы для решения повседневных задач в области информационной безопасности [РБК]:

Обнаружение и предотвращение утечек данных (DLP — data leakage prevention): AI и ML могут быть использованы для анализа образа жизни данных и обнаружения несанкционированного доступа или передачи конфиденциальных данных.

Системы обнаружения событий информационной безопасности (SIEM): AI и ML могут быть использованы для анализа больших объемов журналов событий и данных, связанных с информационной безопасностью, для обнаружения аномальных образов или паттернов, которые могут указывать на угрозы информационной безопасности.

Решения по обнаружению аномальной активности на конечных хостах (EDR, XDR): AI и ML могут быть использованы для анализа образа жизни данных и обнаружения несанкционированного доступа или передачи конфиденциальных данных на конечных хостах, таких как компьютеры и мобильные устройства.

Автоматизация поиска и устранения уязвимостей в системах: AI и ML могут быть использованы для сканирования систем на предмет уязвимостей и планирования их устранения.

Автоматически создает карточку актива, в которой ведется журнал его состояния.

Не дублирует активы при изменении IP- или MAC-адреса — благодаря идентификации по дополнительным параметрам (тип ОС, имя сетевого узла, признак виртуальности узла).

Для обучения нейронной сети нам нужны данные скорости ввода символов с клавиатуры, движения курсора по экрану, какие действия совершает пользователь, как только входит в систему, в какие папки он заходит или каким браузером он пользуется. Также нужны IP-адреса пользователей, в случае, если пользователь работает удаленно, чтобы в случае смены страны или города была возможность отключить этого пользователя.

«С помощью мониторинга показателей поведения пользователя при работе с информационными системами (скорость работы на клавиатуре, перемещение мышки и т.д.) системы поведенческого анализа способны выявить, что компьютером пользуется злоумышленник и сообщить о необходимости принятия соответствующих мер», — дополняет партнер, лидер практики технологического консультирования компании ДРТ Тимофей Хорошев.

Функции искусственного интеллекта в информационной безопасности могут быть различными, но некоторые из наиболее распространенных функций включают [Сбербанк]:

Отправка уведомлений аналитику ИБ: если искусственный интеллект обнаруживает аномалии в поведении пользователя, он может отправить уведомление аналитику информационной безопасности, чтобы тот мог провести дальнейшее расследование.

Отключение или блокировка функций пользователя: если искусственный интеллект подозревает, что пользователь пытается взломать систему или совершить какие-либо другие незаконные действия, он может отключить или заблокировать функции пользователя, чтобы предотвратить возможные угрозы.

Автоматическое обновление системы: искусственный интеллект может обновлять систему автоматически, чтобы защитить ее от новых угроз.

Автоматическое удаление вредоносных программ: искусственный интеллект может удалять вредоносные программы автоматически, чтобы защитить систему от их угроз.

В целом, AI и ML предлагают новые возможности для обнаружения и предотвращения угроз информационной безопасности, автоматизации процессов защиты данных и улучшения эффективности систем информационной безопасности. Использование AI и ML в этой области все еще находится в стадии развития, и многие из этих методов все еще исследуются и улучшаются.

Список источников и литературы:

Рахметов Р. Искусственный интеллект в информационной безопасности // Security Vision. Автоматизированная платформа безопасности. URL: https://www.securityvision.ru/blog/iskusstvennyy-intellekt-v-informatsionnoy-bezopasnosti (дата обращения: 25.03.2024).

Литвинов Р. Искусственный интеллект в информационной безопасности // Инфобезопасность: блог. URL: https://infobezopasnost.ru/blog/articles/iskusstvennyj-intellekt-v-informatsionnoj-bezopasnosti/ (дата обращения: 15.03.2024).

Попова И. Как искусственный интеллект повышает кибербезопасность // РБК. Новая экономика. Новости. 2023. 16 нояб. URL: https://www.rbc.ru/neweconomy/news/6554cc119a79477fa20d3dda (дата обращения: 20.03.2024).

Как ИИ помогает кибербезопасникам бороться с киберпреступниками // Сбербанк. URL: http://www.sberbank.ru/ru/person/kibrary/articles/kak-iskusstvennyj-intellekt-pomogaet-kiberbezopasnikam-borotsya-s-kiberprestupnikami (дата обращения: 22.03.2024).

УДК 002.1:004.8

М. Э. Рзаев[1]

Российский государственный профессионально-педагогический университет

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СРАВНЕНИИ ДОКУМЕНТОВ

Аннотация. В работе рассматривается применение искусственного интеллекта в процессе сравнения документов на предприятиях.

[1] Научный руководитель: С. В. Ляхов, кандидат технических наук, доцент, заведующий кафедрой РГППУ.