gkreshenie.ru/blog/2021/08/10/1c-abby-comparator-cravnenie-dokumentov-i-vyyavlenie-znachimyh-nesootvetstvij/ (дата обращения: 14.04.2024).

УДК 005.922.1:004.8

Р. В. Тихолаз[1]

Российский государственный профессионально-педагогический университет

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Аннотация. С увеличением объема информации, цифровизацией процессов и расширением возможностей технологий, угрозы для конфиденциальности и целостности данных значительно возросли. В этом контексте документооборот, являющийся жизненно важным элементом для многих предприятий и организаций, требует особого внимания в плане обеспечения информационной безопасности. В данной работе будет рассмотрена возможность использовать нейронные сети для поддержания безопасности электронного документооборота.

Ключевые слова: нейронные сети, информационная безопасность, искусственный интеллект, электронный документооборот

В наше время информационная безопасность стала одним из важнейших аспектов любого организационного процесса. Традиционные методы обеспечения информационной безопасности, такие как шифрование, аутентификация и авторизация, являются необходимыми, но недостаточными для борьбы с современными угрозами. Атаки становятся все более изощренными, а защитные механизмы — все более уязвимыми [Дзен].

Появляется необходимость использования нейронных сетей в качестве дополнительного инструмента для обеспечения информационной безопасности документооборота. Нейронные сети имеют уникальные возможности в обнаружении аномалий и атак, основанных на нестандартных или аномальных паттернах в поведении пользователей или внутренних процессах системы.

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

Целью работы является обеспечение безопасности документооборота на основе нейронных сетей.

Преимущества использования нейронных сетей и их возможности [Хабр]:

Обнаружение аномалий: Нейронные сети могут обучаться на больших объемах данных и выявлять аномалии в поведении пользователей или в документообороте, что помогает предотвращать утечки информации или несанкционированный доступ.

Автоматизация: Алгоритмы машинного обучения позволяют автоматизировать процесс мониторинга и обнаружения угроз, снижая трудозатраты на администрирование системы информационной безопасности.

Адаптивность: Нейронные сети способны адаптироваться к новым угрозам и изменениям в окружающей среде, что делает их эффективными инструментами для защиты информации в быстро меняющемся цифровом мире.

Обнаружение фишинга: Нейронные сети могут анализировать текстовые и графические данные электронных писем и идентифицировать попытки фишинга или мошенничества.

Мониторинг доступа: Путем анализа журналов доступа нейронные сети могут выявлять несанкционированные попытки доступа к конфиденциальным документам или системам.

Оптимизация политик безопасности: Алгоритмы машинного обучения могут помочь оптимизировать политики безопасности на основе анализа поведения пользователей и обнаруженных угроз.

Использование нейронных сетей и искусственного интеллекта в безопасном электронном документообороте:

Многие компании в сфере информационных технологий и кибербезопасности активно используют нейронные сети для улучшения защиты информации и обеспечения безопасности документооборота. Вот несколько примеров [Rspectr]:

Google: Компания использует машинное обучение и нейронные сети для повышения безопасности своих сервисов, включая Google Workspace. Эти технологии применяются для фильтрации спама и фишинговых писем в Gmail, а также для обнаружения и предотвращения несанкционированного доступа к документам в Google Drive.

Microsoft: В рамках Microsoft 365 и Azure компания использует машинное обучение для анализа поведенческих паттернов пользователей и обнаружения потенциально опасных действий, что помогает предотвратить утечки данных и атаки на информационные системы.

Symantec (часть Broadcom): Symantec использует машинное обучение для обеспечения защиты конечных точек и обнару-

жения угроз на основе поведения. Это включает анализ трафика данных и действий пользователей для выявления потенциальных угроз безопасности.

Darktrace: Эта компания предлагает продукты кибербезопасности, основанные на искусственном интеллекте, которые автоматически обнаруживают и реагируют на угрозы в реальном времени. Darktrace использует нейронные сети для моделирования «нормального» поведения в сети компании и быстрого обнаружения отклонений.

Palo Alto Networks: Компания разрабатывает средства кибербезопасности, которые включают применение машинного обучения для защиты от угроз. Их решения используют нейронные сети для анализа трафика и выявления скрытых угроз, таких как неизвестные до этого вирусы или атаки zero-day.

IBM: В рамках своего продукта IBM Security использует нейронные сети и другие методы машинного обучения для защиты данных и документооборота. Они анализируют поведенческие модели и могут предсказывать потенциальные угрозы до того, как они произойдут.

Использование нейронных сетей в обеспечении информационной безопасности документооборота представляет собой перспективное направление развития. Эти интеллектуальные системы обладают потенциалом для значительного улучшения защиты информации и снижения рисков для бизнеса. Однако следует помнить, что нейронные сети не являются панацеей и должны применяться в комбинации с другими методами обеспечения информационной безопасности для достижения наилучших результатов.

Список источников и литературы:

Александра Мурзина, руководитель отдела перспективных технологий Positive Technologies // Дзен. URL: https://dzen.ru/a/Zc8XKFI15nBNx7-C (дата обращения: 20.03.2024).

Нейронные сети в кибербезопасности // Хабр. URL: https://habr.com/ru/articles/587694/ (дата обращения: 12.03.2024).

Как нейросети борются с хакерами // Rspectr. Сатьи. 2023. 14 авг. URL: https://rspectr.com/articles/kak-nejroseti-boryutsya-s-hakerami (дата обращения: 15.03.2024).