**УДК 004.852**

# СЕРВИС ВЫЯВЛЕНИЯ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

**Бондаренко Л.А.** (Военно-космическая академия А.Ф. Можайского)
**Научный руководитель – к.т.н. Менисов А.Б.**
(Военно-космическая академия А.Ф. Можайского)

В данной работе рассматривается решение проблемы утечки персональных данных в открытых источниках информации (сети Интернет и социальных сетях) и ее своевременной нейтрализации. Описывается архитектурное решение для сервиса, в основе которого лежит нейронная сеть, способная в режиме реального времени сканировать открытые источники для выявления персональных данных.

**Введение.** Цифровая трансформация экономики предоставляет широкий спектр возможностей и преимуществ, но также способствует повышению угрозы утечки персональных данных. Парирование данной угрозы заключается в поиске и дальнейшем удалении или замене персональных данных в открытых источниках. Современный уровень технологий предоставляет широкий спектр технологий автоматизированных процессов парирования утечки персональных данных, однако, в зависимости от языка, типа данных и других факторов задача остается сложной. Появление новых нейросетевых моделей за последние годы привело к значительным улучшениям в области обработки естественного языка.

**Основная часть.** В рамках исследования был проведен анализ возможных путей снижения угрозы утечки персональных данных и определен оптимальный подход. Выбранная архитектура нейросетевой модели (рекуррентная модель с долгой краткосрочной памятью) позволяет достичь лучшего качества выявления из-за ее адаптивности к тексту при длинном контексте (затухании градиентов).

На основе нейросетевой модели разработан сервис парирования утечек персональных данных с масштабируемой микросервисной архитектурой со следующим функционалом:

−обеспечением децентрализованного управления информационной защиты персональных данных организации, обращения к ресурсам со всех устройств;

−сбором данных как с отдельных web-страниц и web-документов, так и из социальных сетей и мессенджеров;

−классификацией типа персональных данных (ФИО, должность, контактная информация, места работы и учебы и т.д.);

−возможностью формирования отчетных документов о проведении мониторинга.

**Выводы.** Практическая значимость заключается в возможности применения сервиса при обосновании и разработке организационно-технических решений информационной безопасности