УДК004.8

ФУНКЦИОНАЛЬНЫЙ ОБЛИК ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ НАБЛЮДЕНИЯ ЗА НАЦИОНАЛЬНЫМ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ

Тельбух В. В. (адъюнкт 61 кафедры ВКА имени А.Ф. Можайского)
Научный руководитель –
Бирюков Д.Н. (д.т.н., доцент, начальник 61 кафедры ВКА им. А.Ф. Можайского)

Аннотация

В работе проведен анализ состояния национального информационного пространства Российской Федерации. Выявлены тенденции смещения угроз национальной безопасности в информационную сферу. Обоснована необходимость создания интеллектуальной информационной системы поддержки принятия решений органов военного и гражданского управления в условиях динамически изменяющейся информационной обстановки и попыток деструктивного информационно-психологического воздействия на пользователей интернет-ресурсов в целях навязывания им ошибочного представления о текущих ключевых событиях в различных сферах деятельности государства. Сформулированы основные требования к системе интеллектуального наблюдения за единым национальным информационным пространством.

Введение

Спецслужбы иностранных государств и террористические организации проводят информационно-пропагандистские кампании для дестабилизации внутриполитической и социальной ситуации в различных регионах мира, в целях смещения неугодных политических режимов. Отчетливо видны попытки подорвать внутриполитическую стабильность в России, путем провокаций и усиления протестных настроений местного населения в отношении руководства страны. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, при этом широко используются возможности сетевых информационных технологий. В качестве одного из примеров, демонстрирующих использование иностранными государствами подконтрольных СМИ и сетевых ресурсов, можно привести распространение Facebook, Instagram, Twitter и YouTube недостоверной информации о ходе антиправительственных акций на Болотной площади в Москве в 2011-2012 годах, что способствовало усилению протестной активности митингующих, в том числе за счет вливания в их ряды новых участников, поверивших дезинформирующим публикациям. В связи с чем экспертами обозначены тенденции смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации.

Основная часть

Выявление информационных угроз и идентификация попыток манипулирования общественным мнением по средствам сетевых технологий лежит в компетенции экспертов-аналитиков различных силовых ведомств, таких как Министерство обороны Российской Федерации, Федеральная служба безопасности, Министерство внутренних дел и др. Однако с ежегодным ростом количества информационных ресурсов обработка массива публикуемой информации становится все более сложной задачей, требующей перехода от качественных экспертных оценок, по результатам изучения материалов информационных сообщений, к автоматизированным методам, что позволит повысить объективность статистических показателей за счет увеличения объемов обрабатываемой информации, а также снизить субъективизм экспертов в оценивании ситуации.

Таким образом, очевидна потребность в создании интеллектуальной информационной системы поддержки принятия решений органов военного и гражданского управления в условиях динамически изменяющейся информационной и политической обстановки, а также попыток негативного информационно-психологического воздействия на персонал

организационно-технических систем, а также аудиторию различных интернет-сообществ путем применения сетевых информационных технологий.

По итогам анализа тенденцией использования информационного пространства в качестве среды деструктивного вмешательства во внутренние сферы деятельности государства и задач, возлагаемых на профильные подразделения и государственные органы управления, в статье предложены основные требования к системе интеллектуального наблюдения за национальным информационным пространством с использованием технологий искусственного интеллекта:

на уровне мониторинга и обработки информационных потоков:

поиск в режиме реального времени публикаций в различных интернет-СМИ, тематических сообществах, блогах, форумах, сервиса обмена фото и видео контентом, социальных сетях и тематических площадках по ключевым словам, согласно тезаурусу информационных угроз, и обработка полученных данных на предмет выявления в них негативной тональности;

фиксация аномальных изменений в информационной обстановке (в открытых источниках информации) на основе анализа скорости распространения потенциально опасных негативных публикаций и их количества;

извлечение данных об источниках информации (название ресурсов, название публикаций и их содержание, время публикации, авторы, количество позитивной и негативной реакции аудитории, количество просмотров, охват аудитории информационных ресурсов и другой информации в зависимости от типа источника);

сбор данных о динамике распространения потенциально опасных публикаций среди пользователей интерент-ресурсов.

на уровне моделирования информационной обстановки:

классификация негативной информации и ее носителей по уровню влияния на информационную обстановку, формирование и дополнение базы знаний;

идентификация первоисточников и центров влияния на формирование мнения у аудитории, установления их связей с другими участниками сетевых сообществ, вовлеченных в распространения потенциального опасного контента в открытых источниках информации, способного дестабилизировать обстановку внутри страны;

моделирование сценариев распространения информационных угроз в открытых источниках информации на основе установленных топологических связей между первоисточниками, их сетью распространения, центрами сетевого влияния на мнения аудитории.

Заключение

Видится, что система интеллектуального наблюдения за национальным информационным пространством с использованием технологий искусственного интеллекта, в которой будут реализованы предложенные в работе функциональные возможности, сможет позволить:

повысить полноту и объективность анализа и оценивания информационной, политической, военной, социальной обстановки и обстановки других сфер в жизни государства и общества;

обнаруживать признаки целенаправленного негативного информационно-психологического воздействия на пользователей телекоммуникационных сетей на начальных этапах проведения;

идентифицировать и отслеживать потенциально вредоносную активность реальных и потенциальных центров влияния на мнения пользователей социально-сетевых ресурсов;

выработать рекомендации для системы управления и принятия решений по предотвращению или снижению последствий деструктивного воздействия посредствам потенциально опасного контента.