3. *Степанцов М.Е.* Моделирование некоторых сценариев информационного противоборства при помощи клеточного автомата / Проектирование будущего. Проблемы цифровой реальности: труды 5-й Международной конференции (3-4 февраля 2022 г., г. Москва). – М.: ИПМ им. М.В. Келдыша, 2022. – С. 205-214.

4. *Тоффоли Т., Марголус Н.* Машины клеточных автоматов. – М: Мир, 1991. – 283 с.

5. *Новиков А.С.* Атомизация общества и её роль в становлении «общества масс» // Теория и история. – 2009. – № 2. – С. 192-197.

DOI: 10.25728/iccss.2022.76.66.034

Исхакова А.О.

Детектирование разнородных проявлений кибератак на примерах анализа веб-ресурсов

Аннотация: В работе авторами поднимается вопрос анализа электронного текстового и медиаконтента с целью выявления кибератак. Рассматривается пласт кибератак, характеризующийся использованием виртуальной среды, сети Интернет, различных онлайн-инструментов для осуществления неправомерных действий. Обозначено направление обработки и анализа перечисленных средств для детектирования проявлений кибератак на основе эмоционального воздействия на пользователя.

Ключевые слова: кибератака, Интернет, веб-ресурс, виртуальная среда, анализ данных, эмоциональное воздействие, Интернет-контент

В последние годы влияние виртуальной среды на человека выросло в разы. На это повлияли многократный рост ресурсов, вовлеченность всех сфер жизни, бизнеса, социальных институтов в онлайн формат, привлекательность создаваемого контента. Вместе с масштабом Интернет-среды выросла и его значимость для человека – его потребителя [1, 2]. Веб-ресурсы, а также ресурсы на основе популярных мессенджеров, на сегодняшний день, являются основным методом как информирования населения, так и воздействия на него. Возможность сокрытия авторства, отсутствие

строгих канонов представления информации, доступность как с точки зрения формирования контента, так и с точки зрения потребления, – факторы, которые позволяют говорить о высоком потенциале виртуальной среды как средства воздействия на человека, манипуляции и обмана.

Многими специалистами используется достаточно радикальное определение совокупности описанных процессов – «информационная война» [3, 4]. Если говорить о формах воздействия в Интернете, то нельзя назвать их жестокими и бесчеловечными (как подразумевает упомянутое определение). Однако присущие в данном случае массовость, сложность детектирования и блокирования, разнообразие реализаций позволяют сегодня констатировать в этой связи серьезную угрозу для государства.

Исследование данного направления показало, что перспективными являются несколько направлений детектирования проявлений угроз через воздействие на пользователей в виртуальной среде:

1) оценка процессов функционирования сообществ социальных сетей;

2) оценка эмоциональной составляющей содержимого виртуального контента;

3) оценка воздействия конкретных проявлений контента (цвет, частота звука, шрифт и т.д.);

4) экспертное формирование перечня рубрик, с использованием которых воздействие наиболее вероятно.

Например, цикл работ [5-7] по созданию динамической системы функционирования сообществ социальной сети показал, что ресурсу присуще характерное изменение выделенных показателей в разные периоды. Например, размещение нового контента закономерно порождает всплеск ответных действий пользователей. Но при этом факты искусственной активизации и «раскрутки» заданной темы показывают характерные изменения графиков поведения аудитории.

В работе [8] представлен результат оценки воздействия звуковых частот на оператора (слушателя) с целью выявления возможных реакций. Сравнительная таблица оценок информативности рассмотренных время-частотных преобразований для анализа паттернов пользовательских показателей показала, что определенные частоты заставляют чувствовать пользователя

усталость или наоборот бодрость. Однако сложность оценки биомедицинских сигналов не позволяет повсеместно применять такой подход в исследуемой задаче.

Подход на основе оценки эмоциональной составляющей Интернет-контента предоставил наибольший потенциал в части автоматизации процесса детектирования исследуемых кибератак. В связи с гетерогенностью электронных материалов следует исследовать каждый из них, но сначала по отдельности, а в дальнейшем объединять результаты. Применение методов машинного обучения, в частности нейронных сетей, позволяет сегодня говорить о возможности достаточно эффективной классификации медиафайлов по признаку наличия эмоции. Например, при исследовании изображений с целью выявления деструктивного Интернет-контента по одному кадру [9] удалось показать точность классификации не ниже 80 %, по всем классам при тестировании на заранее размеченной коллекции. В работе [10] показаны идентичные исследования по голосовому (аудио) материалу.

Задача классификации разнородного контента, распространяемого в сети, во многом является слабоформализованной. Процессы в сообществах социальных сетей зачастую зависят от множества неоцениваемых факторов. Разбиение на классы субъективно. Проявление эмоций или форм воздействия можно оценить как многоликое и сложно учитываемое. Все эти факторы объясняют наличие множества направлений исследований для решения задачи выявления кибератак в контенте социальных сетей, а также трудоемкость их компоновки. При этом применение методов машинного обучения позволило достичь высоких результатов классификации медиаконтента – обнаружения материалов агрессивного содержания – до 80 %, что говорит о перспективности данного подхода.

Исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук МК-3172.2021.1.6

Литература:

1. *Казарин О.В., Скиба В.Ю., Шаряпов Р.А.* Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2016. – № 1(3). – С. 54-72.

2. *Власенко М.С.* Обеспечение информационной безопасности несовершеннолетних в сети интернет: современное состояние и совершенствование правового регулирования // Вестник Волжского университета им. В.Н. Татищева. – 2019. – Т. 1. № 3. – С. 98-105.

3. *Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.* Информационные войны и социальные сети // Информационные войны. – 2010. – № 3 (15). – С. 44-53.

4. *Фролов Н.В.* Социальные сети как инструмент ведения информационных войн // Социодинамика. – 2018. – № 8. – С. 1-6.

5. *Охапкина Е.П., Охапкин В.П., Мещеряков Р.В., Исхакова А.О., Исхаков А.Ю.* Динамическая система функционирования сообществ социальной сети // Известия Кабардино-Балкарского научного центра РАН. – 2022. – № 2 (106). – С. 41-71.

6. *Охапкина Е.П., Мещеряков Р.В., Исхакова А.О., Исхаков А.Ю.* К вопросу устойчивости динамической системы функционирования сообществ социальной сети // Вестник КРАУНЦ. Физико-математические науки. – 2022. – Т. 38. № 1. – С. 106-130.

7. *Охапкина Е.П., Роганов А.А.* Управляющие воздействия в социальных сетях: аспекты выявления / Комплексная защита информации. Материалы XXVI научно-практической конференции. Ответственный за выпуск Касанин С.Н. – Минск: И.Сивчиков, 2021. – С. 192-195.

8. *Iskhakova A.O., Alekhin M.D., Bogomolov A.V.* Time-frequency transforms in analysis of non-stationary quasiperiodic biomedical signal patterns for acoustic anomaly detection // Информационно-управляющие системы. – 2020. – № 1. – С. 15-23.

9. *Русаков К.Д., Исхакова А.О., Мещеряков Р.В.* Распознавание деструктивного мультимедиаконтента в социокиберфизической системе мониторинга сети интернет по одному кадру // Нейрокомпьютеры: разработка, применение. – 2022. – Т. 24. № 3. – С. 5-17.

10. *Iskhakova A.O., Wolf D.A., Galin R.R., Mamchenko M.V.* 1-D

convolutional neural network based on the inner ear principle to automatically assess human's emotional state // E3S Web of Conferences. – 2020. – Vol. 224. – P. 1-10.

DOI: 10.25728/iccss.2022.95.50.035

Асратян Р.Э.

Подход к созданию защищенных сетевых туннелей в распределенных системах на основе Cryptographic Message Syntax (CMS)

Аннотация: Рассмотрен новый подход к построению защищенных каналов (туннелей) через общедоступную сеть, основанный на использовании технологии Cryptographic Message Syntax (CMS) для инкапсуляции информационных запросов в структуру т.н. «защищенного сообщения». Показано, что, в отличие от известных подходов, предложенная организация защищенного туннеля позволяет ему гибко настраиваться на работу с любой криптосистемой, поддерживающей стандарт CMS, прямо в ходе работы без какой-либо доработки и/или конфигурирования.

Ключевые слова: распределенные системы, VPN, информационная безопасность, web-сервисы, разграничение прав доступа, маршрутизация запросов

Так как почти все современные территориально-распределенные информационные системы используют Интернет для организации взаимодействия удаленных друг от друга рабочих станций и серверов, задача защиты данных в общедоступной сети уже давно находится в центре внимания разработчиков [1, 2]. Разумеется, возможно интегрировать крипто-средства и защищенные сетевые протоколы непосредственно в клиентские и сервисные компоненты системы. Однако такое решение весьма трудоемко, а цена ошибки в данной области может быть высока. Поэтому, обычный способ решения этой задачи заключается в использовании технологии VPN (Virtual Private Network), в качестве готового решения, позволяющего реализовать защищенный «туннель» через общедоступную сеть [3, 4]. Так как средства криптозащиты