МИНОБРНАУКИ РОССИИ

Федеральный исследовательский центр «Информатика и управление» РАН
Национальный комитет РАН по распознаванию образов
и анализу изображений
Институт информационных технологий Министерства науки и образования
Азербайджанской Республики
Институт проблем передачи информации им. А. А. Харкевича РАН
Белорусский государственный университет
Национальный исследовательский Томский государственный университет
Федеральный исследовательский центр «Карельский научный центр РАН»
Ошский государственный университет
Юго-Западный государственный университет

ОПТИКО-ЭЛЕКТРОННЫЕ ПРИБОРЫ И УСТРОЙСТВА В СИСТЕМАХ РАСПОЗНАВАНИЯ ОБРАЗОВ И ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Распознавание – 2023

Сборник материалов XVII Международной
научно-технической конференции

12–15 сентября 2023 года

Курск
ЮЗГУ
2023

УДК 004.056

Б. Р. Набиев[1], К. Г. Дашдамирова[1]
e-mail: Babek.nabiyev@gmail.com, konulahmed@gmail.com

[1]Институт информационных технологий, г. Баку, Азербайджанская Республика

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ КИБЕРУГРОЗ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Исследованы технологии интеллектуального анализа киберугроз (Cyber Threat Intelligence – CTI). Исследованы проблемы в этой области, показана необходимость интеллектуального анализа киберугроз на основе технологий искусственного интеллекта.

В настоящее время в глобализированном мире широкое распространение получили использование и применение Интернета и реализуемых через него услуг. Поэтому злоумышленники создают киберугрозы и осуществляют кибератаки, используя различные методы и инструменты. С этой целью используются многочисленные методы безопасности для обнаружения и предотвращения кибератак. Однако значительный рост числа, разнообразия и сложности образцов вредоносных программ в последние годы делает традиционные подходы к обеспечению безопасности неэффективными перед лицом кибератак нового поколения. Организованная киберпреступность стала глобальной проблемой и является одной из актуальных проблем для всех стран мира. В 2022 г. ущерб от киберпреступности во всем мире составил около 8,4 трлн долл. США. Прогнозируется, что к 2023 г. ущерб от незаконной деятельности в интернете превысит 11 трлн долл. США [1] .

Злоумышленники сотрудничают друг с другом, совместно используют различные инструменты и сервисы, обмениваются опытом на определенных платформах, и это еще больше повышает эффективность кибератак. В таких условиях получение любой информации о вредоносном поведении и используемых им методах очень важно как для их предотвращения, так и для борьбы с ними. Cyber Threat Intelligence (CTI) – область кибербезопасности, сформированная на основе технологий искусственного интеллекта, направленных на сбор, анализ и разрешение информации о текущих и потенциальных атаках, угрожающих безопасности организации или ее активов.

В зависимости от исходных требований, источников данных, целей и области применения CTI в основном реализуется на четырех уровнях: стратегическом, тактическом, технологическом и оперативном [4].

Стратегический уровень – это обобщенный анализ потенциальных кибератак и их возможных последствий для лиц, принимающих решения. Он представлен в виде официальных документов, отчетов и презентаций и

основан на подробном анализе рисков и тенденций со всего мира. Он используется для составления высокоуровневого представления о ландшафте кибербезопасности организации.

Тактический уровень предоставляет информацию о тактике и технологических процедурах, используемых злоумышленниками. Этот уровень предназначен для специалистов, которые непосредственно занимаются защитой информационных технологий и информационных ресурсов. Предоставляет подробную информацию о том, как организация может быть атакована, на основе лучших способов защиты или смягчения последствий последних используемых атак.

Технологический уровень фокусируется на признаках, указывающих на начало кибератаки, которая включает в себя фишинг, социальную инженерию и другие угрозы. На технологическом уровне социальная инженерия играет важную роль в предотвращении атак. По мере того как злоумышленники обновляют свою тактику, используя новые лазейки и уловки, применяемые технологии также должны адаптироваться к новой реальности.

Оперативный уровень основан на сборе данных из различных источников, включая операционные системы, сеть, журналы и многое другое. Используется для прогнозирования характера и времени будущих атак. Методы интеллектуального анализа данных и машинного обучения часто используются для автоматизации обработки сотен тысяч данных на нескольких языках [2].

Помимо того, что это новый подход, CTI также имеет ряд актуальных проблем [3]: определение вектора атаки; обнаружение индикатора атаки; определение приоритетов корпоративной безопасности; кибербезопасность сотрудников, а также важная интеллектуальная собственность и корпоративные данные должны быть защищены.

В эпоху современных информационных технологий необходимо разрабатывать новые подходы для предотвращения постоянного роста кибератак. Эффективное использование CTI решений позволит специалистам по кибербезопасности создавать надежные механизмы защиты от новейших угроз. Для предотвращения угроз в быстро развивающейся киберсреде планируется применять методы искусственного интеллекта на основе подхода CTI.

СПИСОК ЛИТЕРАТУРЫ

1. Estimated cost of cybercrime globally 2016-2027 // Statista: [site]. URL: https://www.statista.com/statistics/1280009/20 (дата обращения: 04.04.2023).

2. Cyber threat intelligence sharing: Survey and research directions / T. D. Wagner, K. Mahbub, E. Palomer, A. Abdallah // Computers & Security. 2019. Vol. 87. P. 101589.

3. Conti M., Dargahi T., Dehghantanha A. Cyber threat intelligence: challenges and opportunities. Springer International Publishing, 2018. P. 1–6.

УКД 004.77

Д. С. Нестуев[1], Д. Б. Борзов[1]
e-mail: nestruev98@mail.ru

[1]Юго-Западный государственный университет, г. Курск, Российская Федерация

ИСПОЛЬЗОВАНИЕ БЕСПРОВОДНОГО ВЫЧИСЛИТЕЛЬНОГО КЛАСТЕРА ПРИ ОБРАБОТКЕ ИЗОБРАЖЕНИЙ

В области обработки изображений все более распространенным становится использование беспроводных вычислительных кластеров. Использование беспроводного вычислительного кластера в обработке изображений дает несколько преимуществ, таких как повышенная скорость и повышенная точность.

Одним из наиболее значительных преимуществ использования беспроводного вычислительного кластера при обработке изображений является повышенная скорость обработки. Обработка больших изображений может быть трудоемкой задачей, требующей значительных вычислительных мощностей. С беспроводным вычислительным кластером несколько устройств могут работать вместе для одновременной обработки изображения, что значительно сокращает время обработки. Эта повышенная скорость обработки позволяет более эффективно и своевременно анализировать большие наборы данных [1–3].

Еще одним преимуществом использования беспроводного вычислительного кластера при обработке изображений является повышенная точность результатов. Алгоритмы обработки изображений могут быть сложными, а точность результатов может зависеть от качества данных и доступной вычислительной мощности. С помощью беспроводного вычислительного кластера данные могут обрабатываться с использованием нескольких алгоритмов одновременно, что повышает точность результатов. Кроме того, использование беспроводного вычислительного кластера позволяет анализировать большие наборы данных, что может привести к более точным и значимым результатам.

Использование беспроводного вычислительного кластера при обработке изображений также может повысить масштабируемость процесса. По мере роста размера набора данных требования к обработке также возрастают. В кластере беспроводных вычислений к кластеру можно добавить дополнительные устройства для удовлетворения возросших требований к обработке.