АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЛОКАЛЬНО-АДАПТИВНОГО АГЕНТА КИБЕРРАЗВЕДКИ

Войткус И.А., студент гр. 361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В работе представлено описание алгоритмического обеспечения локально-адаптивного Telegram-агента для автоматизации OSINT-разведки. Рассмотрен комплекс из трех алгоритмов: эвристическая генерация псевдонимов с учетом национальных стандартов транслитерации, динамический синтез синтаксических Dork-запросов и трехэтапный алгоритм биометрической верификации на базе нейросетевой модели Facenet. Описанные подходы позволяют автоматизировать сбор цифрового следа в локальном сегменте, обеспечивая высокую точность распознавания и соблюдение требований законодательства Республики Беларусь в области защиты персональных данных.

Ключевые слова. OSINT-разведка, алгоритмы, кибеpразведка, биометрические данные, защита персональных данных.

В современном мире аудит информационной безопасности организации невозможен без применения инструментов OSINT [1]. Хотя часто существующие платформы кибеpразведки демонстрируют низкую эффективность в локальных задачах поиска в странах СНГ из-за лингвистических барьеров и специфики формирования цифрового следа. Разработанный локально-адаптивный агент решает данные проблемы посредством внедрения специализированного алгоритмического обеспечения.

Первым алгоритмов агента является формирование массива потенциальных сетевых идентификаторов субъекта. Разработанный алгоритм эвристической генерации псевдонимов выполняет нормализацию входных данных (ФИО на кириллице) и их транслитерацию в соответствии с национальными правилами транслитерации Республики Беларусь. Далее генерируются сочетания инициалов, фамилии и разделительных знаков (например, f_familia, familia.i). Данный метод помогает подобрать нужный возможный псевдоним для дальнейшего поиска. В результате чего формируется массив возможных никнеймов для автоматической проверки через API социальных платформ и сервисов разработки.

Далее перед агентом стоит задача выявления скрытых метаданных и утечек в открытом документообороте, для чего применяется алгоритм динамического формирования Dork-запросов. Логика алгоритма заключается в синтезе необходимых URL-строк, содержащих специализированные операторы (например, ext:pdf, site:, allintext:). Алгоритм автоматически адаптирует поисковой запрос под целевой домен организации, что позволяет обнаруживать методические материалы, приказы и отчеты, содержащие конфиденциальные сведения об инфраструктуре.

Критически важным компонентом системы является функция распознавание биометрических данных и сравнение их с эталонными значениями. Для этого данный инструмент используется следующий алгоритм: выполняется инициализация лица и происходит выравнивание по линии глаз, что обеспечивает различные варианты распознавания при различных ракурсах съемки, далее подготовленное изображение подается в нейросеть Facenet [2], которая преобразует визуальные признаки в уникальный 512-мерный вектор. Модель обучена с использованием функции потерь Triplet Loss, что дает минимальное расстояние в векторном пространстве для лиц одного человека. На финальном этапе выполняется расчет косинусного сходства между вектором входного изображения и эталонными векторами из данных фотографии предоставленной для поиска (эталонной), данный расчет вычисляется по формуле:

$$S_c(A, B) = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2} \sqrt{\sum_{i=1}^{n} B_i^2}}, \quad (1)$$

где n – размер вектора; A_i и B_i – компоненты сравниваемых векторов.

При превышении установленного порога (Threshold) система подтверждает личность субъекта. Данный подход позволяет минимизировать ложные срабатывания и проводить верификацию в реальном времени. Схема конвейера алгоритмической обработки данных приведено на рисунке 1.

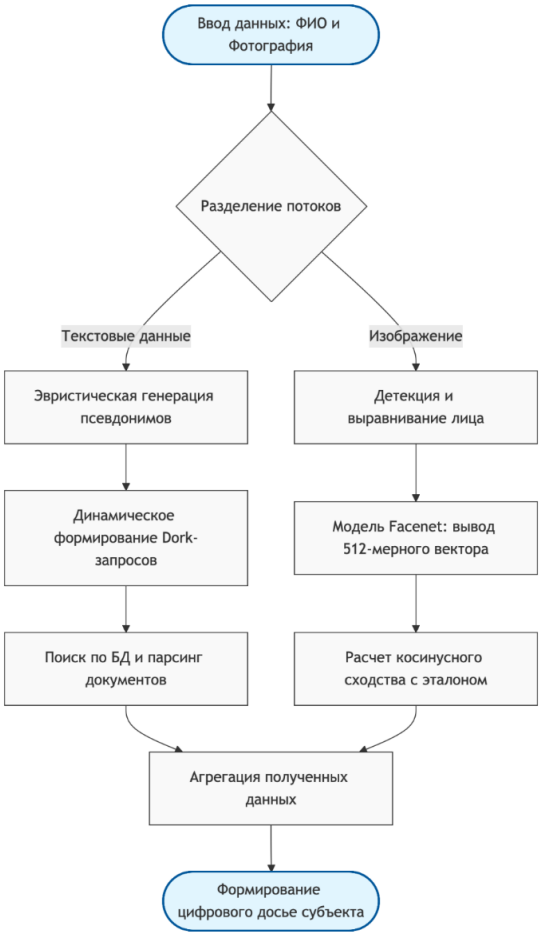

Рисунок 1 – Блок-схема конвейера алгоритмической обработки данных агентом

Перенос процессов OSINT-профилирования из глобальных облачных платформ в локально-изолированные контуры – это не только техническая оптимизация, но и необходимый шаг к достижению подлинного информационной независимости от западных принципов и инстрментов. В настоящее время, когда границы между частным и публичным цифровым присутствием окончательно размыты, способность организации проводить внутренний аудит, не раскрывая сам факт этого аудита внешним игрокам, становится базовым условием выживания инфраструктуры. Данное исследование закладывает фундамент для создания нового поколения локальных систем безопасности, принося в конкретном регионе аудита, максимальную эффективность

Список использованных источников:

1. Войткус И.А. Инструмент для OSINT-разведки и реализации техники MITRIE ATTA&CK T1593 / И.А. Войткус, Е.С. Белоусова // Технические средства защиты информации: матер. XXIV Междунар. науч.-техн. конф., 2026. – С. 342–345.

2. Николенко, С. И. Глубокое обучение. Погружение в мир нейронных сетей / С.И. Николенко, А.А. Кадурин, Е.О. Архангельская. – СПб.: Питер, 2018. – 480 с.