Основные результаты проекта РФФИ 18-07-01488 за 2018 год

В 2018 году исследования проводились в рамках первого этапа Проекта – этапа анализа существующих работ и систем в области сетевой безопасности для построения моделей человеко-машинного взаимодействия базирующихся на сенсорных мультитач-экранах и анализа существующих работ в области когнитивного аппарата человека для построения методики оценки эффективности человеко-машинного взаимодействия и правильной интерпретации последующих результатов.

На этом этапе были получены следующие основные результаты.

1. Проведен анализ научных работ в области визуальной аналитики, в том числе для систем мониторинга безопасности (SIEM), центров оперативного управления безопасностью (SOC) и комплексных систем безопасности. На основе данного анализа составлены: перечень актуальных для сетевой безопасности моделей визуализации, перечень структур данных процессов сетевой безопасности, перечень актуальных для сетевой безопасности способов человеко-машинного взаимодействия. Модели визуализации как и структуры данных подразделены на два типа: модели, способные отображать числовые данные (списки или таблицы) и нечисловые данные (графы и различные связи объектов). Выделены перспективные специфические модели, например: совмещенные модели (рис. 1), модели на основе карт Вороного (рис. 2) и карт деревьев Вороного (рис. 3), диаграммы Корда (рис. 4) и модели на основе гео-карт (рис. 5). Проведен анализ использования методов человеко-машинного взаимодействия в программах анализа сетевой безопасности Wireshark, Zenmap и OSSIM SIEM.

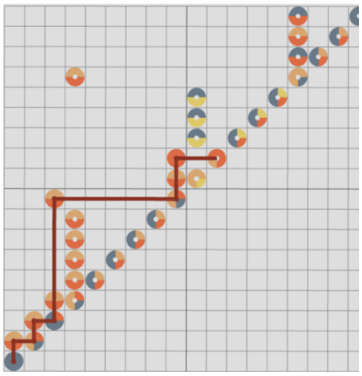

Рис. 1 – Совмещенные модели: модели которые были созданы путем совмещения множества других моделей. На рисунке пример матрицы на основе графов атак где в качестве ячеек матрицы выступает модель на основе глифов.

Рис. 2 – Карты Вороного: модель в которой объекты представлены ячейками, а связи между объектами соприкосновением ячеек. Разделение ячеек разделителем соответствует отсутствию связи. Метрики можно задавать в виде размера, цвета и прозрачности.

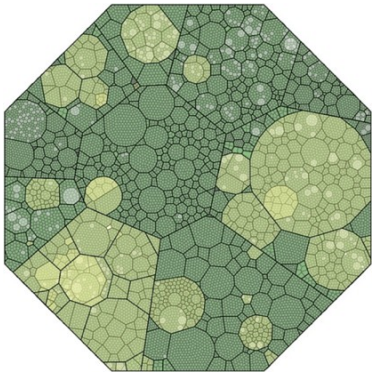

Рис. 3 – Карты деревьев Вороного: состоят из вложенных друг в друга областей, которые можно задавать цветом, размером и прозрачностью. Вложенная структура соответствует иерархии, таким образом Карты Деревьев Вороного могут применяться для иерархических структур.

Рис. 4 – Гео-Карты: вид визуализации в которой модели накладываются на географические карты. На изображении диаграмма Вороного наложена карту Санкт-Петербурга. Расстояние от любого объекта внутри многоугольника до точки на основе которого данный многоугольник был построен всегда меньше, чем до другой точки. Данное изображение сформировано на основе координат базовых станций сотой связи сети Мегафон на Петроградском острове. Таким образом путем эксплуатации уязвимости SS7, получив CellId абонента можно узнать область в которой человек находится.

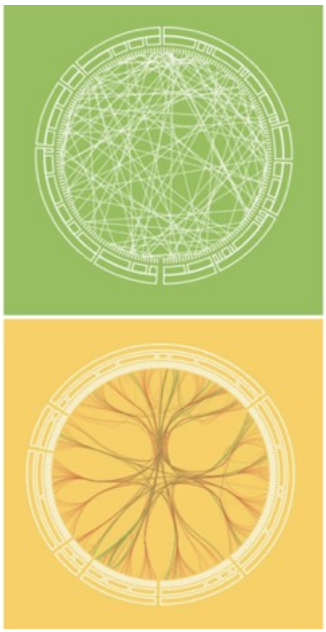

Рис. 5: Диаграммы Корда - торовидная модель в которой внешний контур представляв радиальным графом, а внутренняя обычными связями.

2. Разработана классификация моделей визуализации применяемых для визуальной аналитики сетевой безопасности на основе типа структуры процессов безопасности. Предложена классификация существующих моделей человеко-машинного взаимодействия на основе шаблона визуального поиска. Сформирована классификация данных процессов сетевой безопасности, которые подвергаются визуальной аналитике на основе типов структур данных. Проведены комплексная систематизация и анализ способов человеко-машинного взаимодействия для моделей визуализации в рамках визуальной аналитики данных процессов безопасности.

3. Разработаны новые модели человеко-машинного взаимодействия, базирующиеся на сенсорных мультитач-экранах и на основе жестов оператора, моделей визуализации, структур данных процессов обеспечения сетевой безопасности и системе методов человеко-машинного взаимодействия.

4. Произведен анализ научных работ в области когнитивной графики и когнитивного аппарата человека. Разработана методика оценки эффективности человеко-машинного взаимодействия на основе проведенного анализа.

5. Кроме того, **проанализированные модели визуализации были реализованы для решения задач мониторинга сетевой безопасности**, обнаружения атак, анализа защищенности и сетевых расследований.