Сведения о ходе выполнения проекта по соглашению
No 05.607.21.0322 от «04» декабря 2019 г.
первый этап (2019 год)

Тема: Разработка методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них.

Целью проекта заключается в создании комплекса научных/научно-технических решений, обеспечивающих в условиях обработки трафика сверхвысоких объемов:

- выявление сетевых атак методами аналитического моделирования, вычислительного интеллекта и сигнатурного анализа, а также комбинированными методами;
- защиту от сетевых атак типа отказ в обслуживании, сбор информации и эксплуатация уязвимостей;
- необходимый уровень информационной безопасности и функциональности информационно-телекоммуникационных систем

На **первом** этапе ПНИЭР проведен аналитический обзор современной научно-технической, нормативной, методической литературы, затрагивающей исследуемую научно-техническую проблему, анализировались достигнутые научно-технические результаты в области сбора, предобработки и хранения сетевого трафика сверхвысокого объема, обнаружения сетевых атак на основе сигнатурного анализа трафика, биоинспирированных подходов, аналитического моделирования и машинного обучения, объединения различных подходов к обнаружению сетевых атак, а также выбора контрмер защиты от сетевых атак на основе выявления отклонений в эвристиках трафика сверхвысоких объемов. На основе полученных результатов анализа были сделаны выбор и обоснование направления исследования, сводящееся к решению ряда теоретических и практических задач. Выделены задачи разработки математических методов, моделей и алгоритмов сбора, предобработки и хранения сетевого трафика сетевого трафика сверхвысокого объема, а также практические задачи, заключающиеся в формировании наборов тестовых гетерогенных данных на основе полунатурного моделирования трафика данных и потоков атак в реальном фрагменте компьютерной сети.

Новыми результатами, полученными в ходе исследований на первом этапе, являются:

1 Аналитический обзор современной научно-технической, нормативной, методической литературы, затрагивающей научно-техническую проблему, исследуемую в рамках ПНИЭР.

2 Патентные исследования в соответствии с ГОСТ 15.011-96.

3 Обоснование и выбор направления исследований на основе анализа информационных источников и результатов патентных исследований.

4 Математические методы, модели и алгоритмы сбора и предобработки сетевого трафика сверхвысокого объема, основанных на распределенной параллельной обработке данных.

5 Математические методы, модели и алгоритмы хранения сетевого трафика сверхвысокого объема, обеспечивающих распределенное устойчивое и оперативное хранение информации.

6 Эскизная конструкторская документация (ЭКД) на программно-аппаратный стенд для генерации наборов тестовых гетерогенных данных на основе полунатурного моделирования трафика данных и потоков атак в реальном фрагменте компьютерной сети СГТД.431262.001.

7 Программа и методики (ПМ) экспериментальных исследований программно-аппаратного стенда генерации тестовых наборов гетерогенных данных.

8 Программно-аппаратный стенд генерации наборов тестовых гетерогенных данных на основе полунатурного моделирования трафика данных и потоков атак в реальном фрагменте компьютерной сети.

9 Экспериментальные испытания программно-аппаратного стенда генерации тестовых наборов гетерогенных данных на основе полунатурного моделирования трафика данных и потоков атак в реальном фрагменте компьютерной сети по разработанным Программе и методикам испытаний.