**Соглашение о предоставлении субсидии: 14.578.21.0231**

**RFMEFI57817X0231**

**Тема:** «Предотвращение сетевых атак на основе технологии больших данных и высокопараллельного эвристического анализа сверхвысоких объемов трафика в магистральных сетях Интернет».

**Приоритетное направление:** Информационно-телекоммуникационные системы.

**Критическая технология:** Технологии и программное обеспечение распределенных и высокопроизводительных вычислительных систем.

**Индустриальный партнер:** Общество с ограниченной ответственностью «НеоБИТ»

**Цель проекта:**

Разработка комплекса программно-технических решений, направленного на создание программного комплекса, обеспечивающего:

1.1 выявление сетевых атак методами обнаружения отклонений в трафике сверхбольших объемов, поступающем с пограничных маршрутизаторов магистральных сетей Интернет;

1.2 защиту от сетевых атак типа отказ в обслуживании, атак уровня приложений.

1.3 разработку экспериментального образца программного комплекса обнаружения угроз безопасности информации и защиты от них (далее – ЭО ПК).

**В результате выполнения работ по проекту на первом этапе:**

1. Проведен аналитический обзор современной научно-технической, нормативной, методической литературы, затрагивающей научно-техническую проблему, исследуемую в рамках ПНИЭР, и содержащий сравнительный анализ современных систем обнаружения атак, в том числе, обзор научных информационных источников: статьи в ведущих зарубежных и (или) российских научных журналах, монографии и (или) патенты - не менее 15 научно-информационных источников за период 2011 – 2017 гг.
2. Проведены теоретические мультидисциплинарные исследования существующих методов обнаружения угроз безопасности и защиты от них. По итогам анализа информационных источников, перспективным направлением исследований является эвристический анализ, позволяющий обнаруживать некоторые инварианты параметров сетевого трафика, изменение которых свидетельствует о нарушении безопасности.
3. Проведены патентные исследования в соответствии с ГОСТ Р 15.011-96. Патентные исследования показали, что в настоящее время отсутствуют патенты и иные охранные документы, которые могут препятствовать разработке и применению в Российской Федерации новых методов, алгоритмов и средств, обеспечивающих создание технологии предотвращения сетевых атак на основе технологии больших данных и высокопараллельного эвристического анализа сверхвысоких объемов трафика в магистральных сетях Интернет.
4. Выполнены обоснование и выбор направления исследований на основе анализа информационных источников и результатов патентных исследований. Направление дальнейших исследований связано с разработкой новых мультифрактальных и вейвлет-эвристик, позволяющих обнаруживать аномалии в трафике магистральных сетей, а также с разработкой методов прогнозной аналитики и предсказания поведения сетевого трафика для предотвращения сетевых атак.
5. Разработана симуляционная модель применения технологии «больших данных» и методов высокопараллельного эвристического анализа. Модель объединяет все разработанные методы и формально описывает каждый этап процесса.
6. Разработаны методы сбора и предварительной обработки сверхвысоких объемов трафика магистральных сетей Интернет для высокопараллельного анализа:

* метод автоматической классификации сетевого трафика «на лету», заключающийся в отделении P2P-трафика от web-трафика для повышения точности обнаружения сетевых атак;
* метод сокращения размерности сверхвысокого объема сетевого трафика, заключающийся в извлечении параметров сетевых пакетов и использовании иерархически-зависимых окон агрегации;
* метод динамического распределения сверхвысоких объемов трафика между вычислительными узлами гетерогенного кластера.

1. Индустриальным партнером выполнена разработка методов сбора и предварительной обработки сверхвысоких объемов трафика магистральных сетей Интернет для высокопараллельного анализа:

* метод распределенного сбора сверхвысоких объемов сетевого трафика на основе интеллектуального опроса граничных маршрутизаторов магистральной сети;
* метод хранения информации о сетевом трафике на основе автоматического тиринга, обеспечивающий иерархическое хранение данных для дальнейшего анализа.

Полученные на данном этапе результаты будут использованы при разработке экспериментального образца программного комплекса обнаружения угроз безопасности информации и защиты от них. Сведения о ходе выполнения проекта представлены на сайте <http://ibks-project.ru/tier/>.