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

**Научный руководитель:** П.Д. Зегжда

**Соглашение** № 14.578.21.0231 от 26.09.2017, уникальный идентификатор Соглашения RFMEFI57817X0231.

**Срок выполнения работ по проекту: 26.09.2017 – 30.06.2019.**

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

Работы первого этапа выполнения проекта были посвящены выбору направления исследований. Выбранное направление дальнейших исследований базируется на принципах высокопараллельной обработки сетевого трафика, позволяющей анализировать сетевой трафик в режиме реального времени; сокращения размерности сверхвысоких объемов сетевого трафика для повышения скорости обработки; эффективной организации хранения данных с предоставлением максимально быстрого доступа к статистическим параметрам, важным для анализа безопасности; разделения сетевого трафика на трафик P2P-сетей и web-трафик для повышения точности анализа безопасности; использования для обнаружения аномалий в сетевом трафике мультифрактальных и вейвлет-эвристик, учитывающих специфику трафика магистральных сетей и обладающих высокой чувствительностью к аномалиям и устойчивостью к увеличению объемов данных; прогнозирования поведения сетевого трафика и значений его параметров для предотвращения сетевых атак. Для практического отражения результатов дальнейших исследований на втором этапе будет разработан экспериментальный образец программного комплекса обнаружения угроз безопасности информации и защиты от них.

Сведения о ходе выполнения проекта представлены на сайте <http://ibks-project.ru/tier/>.