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 втором этапе:

1. Разработан алгоритм предварительной обработки сетевого трафика (п. 3.7 ТЗ)
2. Разработаны методы предотвращения сетевых атак на основе технологии «больших данных» и высокопараллельного эвристического анализа, обеспечивающие, в соответствии с Указом Президента Российской Федерации от 01.12.2016 №642, противодействие киберугрозам (п. 20 д) Стратегии НТР РФ) (п. 3.8 ТЗ):
   - метод обнаружения аномалий в сетевом трафике на основе оценки мультифрактальных эвристик временных рядов сетевого трафика (п. 3.8.1 ТЗ)
   - метод обнаружения аномалий в сетевом трафике на основе оценки вейвлет-эвристик временных рядов сетевого трафика (п. 3.8.2 ТЗ)
   - метод предупреждения сетевых атак на основе краткосрочного прогнозирования (п. 3.8.3 ТЗ)

Разработанные методы обеспечивают предотвращение сетевых атак, поскольку включают в себя как ранее обнаружение атак за счет использования мультифрактальных и вейвлет-эвристик, способных реагировать даже на незначительные изменения в поведении временных рядов, сформированных из параметров сетевого трафика, так и их предупреждение с использованием прогнозирования.

3. Проведены дополнительные патентные исследования по ГОСТ Р 15.011-96 (п. 5.2 ТЗ)

4. Разработан экспериментальный образец программного комплекса обнаружения угроз безопасности информации и защиты от них (ЭО ПК), для обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных Указом Президента Российской Федерации от 01.12.2016 №642 (п. 3.9 ТЗ).

5. Разработаны Программа и методики исследовательских испытаний (ПМИ-И) и оценки эффективности разработанного ЭО ПК (п. 3.10 ТЗ).

6. Проведены исследовательские испытания разработанного ЭО ПК в соответствии с ПМИ-И, подтверждающие готовность к практическому применению разработанных методов для обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных Указом Президента Российской Федерации от 01.12.2016 №642 (п. 3.11 ТЗ).

7. Проверено соответствие разработанных программно-технических решений требованиям ТЗ, в том числе проверены:

- возможность сбора информации о трафике (п. 3.12.1 ТЗ);
- обнаружение сетевых атак в сверхвысоких объемах трафика магистральных сетей Интернет (п. 3.12.2 ТЗ);
- возможность защиты от обнаруженных сетевых атак (п. 3.12.3 ТЗ);
- возможность динамического распределения задач по обработке сетевого трафика между вычислительными узлами (п. 3.12.4 ТЗ);
- эффективность и качество разработанной симуляционной модели применения технологии «больших данных» и методов высокопараллельного эвристического анализа (п. 3.12.5 ТЗ)

8. Разработан проект технического задания на проведение ОКР по теме: «Разработка высокопроизводительной системы предотвращения сетевых атак на основе технологии «больших данных» и эвристического анализа».

9. Подготовлены рекламные материалы для участия в выставках, в том числе, международных.

10. Принято участие в мероприятиях, направленных на освещение и популяризацию промежуточных результатов ПНИЭР (конференции, семинары, симпозиумы, выставки, в том числе, международные).

11. Проведена поддержка сайта проекта: оплата доменного имени, оплата хостинга, актуализация содержимого.

12. Подготовлены и поданы заявки на регистрацию РИД.

13. Проведены работы по ресурсному обеспечению.

14. Разработаны методы предотвращения сетевых атак на основе технологии «больших данных» и высокопараллельного эвристического анализа, обеспечивающие, в соответствии с Указом Президента Российской Федерации от 01.12.2016 №642, противодействие киберугрозам (п. 20 д) Стратегии НТР РФ (п. 3.8 ТЗ):

- метод автоматической классификации сетевых атак на основе шаблонов атак (п. 3.8.4 ТЗ);
- метод защиты от сетевых атак на основе псевдослучайной смены сетевых адресов (п. 3.8.5 ТЗ);
- метод защиты от сетевых атак на основе блокирования (п. 3.8.6 ТЗ).

15. Проведен анализ полноты решения задач и достижения поставленной цели ПНИЭР (п. 3.13 ТЗ), в том числе:

- обобщение результатов исследований (п. 3.13.1 ТЗ);
- сопоставление анализа научно-информационных источников и результатов теоретических и экспериментальных исследований (п. 3.13.2);
- анализ выполнения требований ТЗ на ПНИЭР (п. 3.13.3);
- оценка полноты решения задач и достижения поставленных целей ПНИЭР (п. 3.13.4);
- оценка эффективности полученных результатов в сравнении с современным научно-техническим уровнем (п. 3.13.5 ТЗ);
- сравнительный анализ разработанных методов и программного обеспечения с мировыми аналогами, подтверждающий их инновационный характер и охраноспособность для реализации приоритетов научно-технологического развития РФ (п. 3.13.6 ТЗ);
- разработка рекомендаций по использованию результатов ПНИЭР в реальном секторе экономики (п. 3.13.7 ТЗ).

16. Разработаны технические требования и предложения по разработке, производству и эксплуатации продукции с учетом технологических возможностей, и особенностей индустриального партнера (п. 3.14 ТЗ).

17. Проведены маркетинговые исследования рынка систем обнаружения сетевых атак и вторжений, пригодных для выявления отклонений в сверхвысоких объемах сетевого трафика магистральных сетей Интернет (п. 3.15 ТЗ).

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