

## АННОТАЦИЯ ПО ПРОЕКТУ

**Государственный контракт № 02.740.11.0659 от «29» марта 2010 г.**

**Тема:** «Создание информационно-телекоммуникационных систем (ИТКС) высокой доступности и защищенности»

**Исполнитель:** Федеральное государственное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный политехнический университет» (ФГБОУ ВПО «СПбГПУ»)

**Ключевые слова:** информационная безопасность, защищенность, доступность, контроль целостности, параметрическая идентификация, динамическая контентная фильтрация, сигнал

### 1. Цель проекта

1. Обеспечение высокой доступности и защищенности информационно-телекоммуникационных систем (ИТКС).

2. В ходе работы создан комплекс технологических методов и средств, направленных на создание ИТКС высокой доступности и защищенности, а именно:

– технология повышения пропускной способности подсистем передачи информации ИТКС на основе адаптивных алгоритмов обработки, протоколов передачи и защиты сообщений;

– технология динамической контентной фильтрации при доступе к информационно-сетевым ресурсам ИТКС;

– технология автоматизации управления информационной безопасностью ИТКС путем непрерывного поддержания цикла контроля целостности информационной среды.

### 2. Основные результаты проекта

В ходе НИР создана модель алгоритмов приема информации, в которой используются спектрально-эффективные сигналы и присутствует аддитивный каналный шум, а также применяется помехоустойчивое кодирование. Представлена методика компьютерного моделирования алгоритмов формирования и приема сигналов, позволяющая получить спектральные и вероятностные характеристики системы передачи информации. Предложена методика расчета вероятностных характеристик системы передачи информации, в которой используются спектрально-эффективные сигналы и помехоустойчивое кодирование при наличии аддитивного гауссовского шума. Энергетический выигрыш при обработке оптимальных спектрально-эффективных сигналов с OFDM методом итеративного декодирования по сравнению с приемом сигналов с OFDM с прямоугольными огибающими на поднесущих без помехоустойчивого кодирования составляет 2–3,4 дБ при  $P_{ош} = 10^{-3}$ – $10^{-4}$ . При этом выигрыш от применения помехоустойчивого кодирования при приеме сигналов с OFDM с прямоугольными огибающими на поднесущих составляет 2,9–3,3 дБ при  $P_{ош} = 10^{-3}$ – $10^{-4}$ .

При использовании метода итеративного декодирования, достоверность приема спектрально-эффективных сигналов с OFDM выше, чем при приеме сигналов с OFDM с прямоугольными огибающими на поднесущих и помехоустойчивым кодированием.

Создана модель алгоритмов приема информации и методика расчета вероятностных характеристик системы передачи информации. Разработана методика формирования правил фильтрации с использованием формального описания политики доступа. Новизна данных решений заключается в том, что предложенные модели позволяют создавать формальное описание информационной среды исполнения политики доступа и сами политики доступа, интегрировать политику доступа и среду ее исполнения, а также определять соответствие состояния информационной среды требованиям политики доступа и выводить состояния информационной среды,

удовлетворяющие требованиям политик доступа.

Построена модель и реализован макет системы автоматического управления информационной безопасностью ИТКС на базе метода контроля целостности ИС ИТКС. Новизна данной системы и реализованных методов по контролю целостности заключается в том, что в их основе используется логическая модель, описывающая и предсказывающая поведение средств защиты в контексте информационной среды ИТКС; задаются отношения эквивалентности между состояниями информационной среды ИТКС в виде простых критериев безопасности и целостности; впервые предложен и внедрен принцип допустимых отклонений вместо контрольного суммирования при проверке целостности систем.

### **3. Назначение и область применения результатов проекта**

Результаты проекта обеспечивают высокую доступность и защищенность информационной среды ИТКС путем разработки новых методов передачи, обработки, хранения и защиты информации.

В частности, предложенный подход к повышению пропускной способности телекоммуникационной системы за счет применения спектрально-эффективных сигналов позволяет в 2–3 раза повысить пропускную способность телекоммуникационных систем и одновременно обеспечить соответствующую защиту информации от несанкционированного доступа. Областью применения данного решения являются разнообразные телекоммуникационные сети.

Решение задач классификации и идентификации контента позволяет вычислять семантику Интернет-ресурсов, создавать многокомпонентные шлюзы доступа, работающие в среде протоколов IP версии 4 (IPv4) и IP версии 6 (IPv6) и реализующие правила фильтрации в соответствии с политиками информационной безопасности. Данные решения применимы в сфере обеспечения информационной безопасности на уровне сетевых служб, включая DNS, LDAP.

Решение задачи по созданию системы управления информационной безопасностью ИТКС позволяет контролировать и управлять параметрами функционирования согласно контексту информационной среды ИТКС с учетом особенностей конкретной информационной среды ИТКС, условий эксплуатации средств защиты, назначения и состава используемого системного и прикладного программного обеспечения, угроз безопасности. Сфера применения найденных решений: мониторинг и аудит безопасности, анализ защищенности ИТКС, удаленное администрирование безопасности ИТКС, сертификация средств защиты и операционных систем.

В целом использование полученных результатов НИР предполагается при создании новых протоколов работы телекоммуникационных беспроводных сетей, при построении новых средств защиты информации на базе контентной фильтрации протоколов сетевого взаимодействия, при построении интеллектуальных систем управления информационной безопасностью ИТКС в таких отраслях как телекоммуникации, сетевые технологии, информационная безопасность.

Коммерциализация проектом не предусмотрена.

### **4. Достижения молодых исследователей – участников Проекта**

В проекте принимал участие молодой исследователь Калинин М.О., к.т.н., доцент. При его непосредственном участии удалось разработать модель системы управления информационной безопасностью, соответствующую мировому уровню в области информационной безопасности, что позволит использовать полученные результаты в разработке систем моделирования безопасности компьютерных систем

### **5. Опыт закрепления молодых исследователей – участников Проекта в области науки, образования и высоких технологий**

