Первый этап выполнения проекта № 19-07-00953 (2019 г.)

"Модели, методики и алгоритмы анализа защищенности программно-аппаратных компонентов беспроводных сенсорных сетей"

Беспроводные сенсорные сети, объединяющие множества встроенных устройств, сенсоров представляют сравнительно новый вид информационно-телекоммуникационных инфраструктур, которые отличаются наличием специфичных угроз информационной безопасности, обусловленных появлением новых классов осуществляемых на такие системы программно-информационных и физических воздействий и требующих новых путей и механизмов защиты. В проведение анализа защищенности в беспроводных сенсорных сетях обосновывается необходимостью обнаружения вторжений в систему, попыток несанкционированной модификации данных и программного кода устройств, атак подмены сенсоров и нарушения аутентичности устройств, атак истощения энергоресурсов устройств и др., а также уведомление о состоянии критически важных параметров сети с учетом семантики предоставляемых ей сервисов.

Цель Проекта – совершенствование подходов, моделей, методик и алгоритмов анализа защищенности программно-аппаратных компонентов беспроводных сенсорных сетей с использованием комплексного подхода к анализу больших объемов данных, поступающих от устройств и сенсоров сети. Проект ориентирован на моделирование, анализ и практическую реализацию средств анализа защищенности беспроводных сенсорных сетей в условиях наличия разнородных и взаимодействующих между собой устройств, использующих беспроводные протоколы передачи данных с учетом повышенных требований к защищенности таких сетей. За первый год выполнения Проекта получены следующие основные научные результаты.

Работа по проекту на первом этапе его выполнения включает проведение анализа и составление обзора научно-исследовательских работ в предметной области исследования, научное обоснование задачи анализа защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях, разработку модели представления беспроводных сенсорных сетей, разработку комбинированной модели нарушителя и классификация атак в беспроводных сенсорных сетях.

Проведен анализ и сделан обзор научно-исследовательских работ в предметной области анализа защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях, включающий более 100 источников научно-технической информации, в том числе научно-технических статей, опубликованных на русском и английском языках по тематике исследований в рецензируемых изданиях трудов конференций, научных журналах по тематике исследований.

Проведено научное обоснование задачи анализа защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях, включающее обоснование актуальности проводимых исследований, формальную постановку задачи исследования и обоснование целесообразности решения задач Проекта.

Разработаны модели представления беспроводных сенсорных сетей, специфицирующие структуру, функциональные и поведенческие особенности сетей и устройств, входящих в их состав. Модели построены на основе JSON-формата, удобного для формирования, модификации и использования данных, как человеком, так и при помощи автоматизированных программных средств обработки данных. Также построены, применяемые, в том числе при экспертном анализе беспроводных сенсорных сетей, модели на основе UML-диаграмм, позволяющих специфицировать, как статическую, так и изменяющуюся во времени структуру сети, сценарии работы сети, протоколы взаимодействия и различные операционные процедуры. Модели представления беспроводных сенсорных сетей предназначены для отображения динамических характеристик и потоков данных в сети, создания верхнеуровневых профилей по настройке параметров узлов, отправке, получению и распознаванию тестовых и сервисных команд в сети. Модели представления предназначены также для проведения анализа сетевых спецификаций, а

также для верификации с использованием автоматизированных средств поддержки процессов принятия решений проектирования, разработки, обеспечения и анализа защищенности сети. Помимо этого модели предназначены также для анализа атакующих воздействий и инцидентов безопасности на уровне манипуляции командами представления с использованием унифицированных команд обращения к узлам беспроводной сенсорной сети, ее данным и предоставляемым сервисам.

Разработана комбинированная модель нарушителя в беспроводных сенсорных сетях. Модель относится к классу аналитических моделей и включает объединенную классификацию и анализ возможных атакующих воздействий, которые нарушитель способен произвести и их особенности. Комбинированный характер модели нарушителя выражается в применении ряда существующих классификаций, используемых при исследовании беспроводных сенсорных сетей, встроенных устройств, систем Интернета вещей и адаптированных под условия БСС. Выделены основные, заложенные в модель нарушителя, отличительные признаки нарушителей безопасности беспроводных сенсорных сетей: тип нарушителя по отношению к инфраструктуре сети; тип доступа нарушителя к устройству с использованием прямых или непрямых каналов; уровень возможностей нарушителя; тип воздействий нарушителя; тип атакующего узла беспроводной сенсорной сети; число устройств - узлов сети, одновременно используемых нарушителем для выполнения атаки; распределенность воздействий атаки; тип механизма беспроводной сенсорной сети, на который направлено воздействие; тип воздействий нарушителя по уровню сетевой модели; цель нарушителя.

Проанализирован оптимальный состав множества показателей доступности, целостности и конфиденциальности данных пользователей беспроводных сенсорных сетей в интересах анализа и обеспечения их защищенности. При этом предложенный состав множества показателей защищенности, подлежащих анализу в интересах оперативного и достоверного управления защитой информации, позволит повысить безопасность информационных ресурсов, хранимых и обрабатываемых в современных беспроводных сенсорных сетях за счет постоянного и полного отслеживания этих текущих показателей в режиме, близком к реальному времени.

В качестве способов практического использования результатов проекта планируется разработать средства для анализа защищенности программно-аппаратных компонентов беспроводных сенсорных сетей. В частности, планируются программные средства, которые на основе анализа спецификаций устройств сети и информации об ожидаемых видах нарушителей, позволят выявить актуальные угрозы информационной безопасности, которые необходимо предотвратить либо минимизировать размер их последствий. Также планируется разработка программных средств для выявления конкретных инцидентов информационной безопасности в динамике с учетом специфики данных, собираемых на узлах беспроводной сенсорной сети и возможных аномалиях в них и атакующих воздействий.

Такие программные средства ориентированы на применение инженерами-разработчиками и операторами информационно-телекоммуникационных комплексов, включающих в свой состав беспроводные сенсорные сети с целью детектирования инцидентов безопасности и повышения защищенности программно-аппаратных устройств; данных, формируемых и обрабатываемых ими; предоставляемых ими функций. Детектирование атак и повышение защищенности планируется достичь за счет применения модельно-методического аппарата и реализации механизмов информационной безопасности в части моделирования нарушителей информационной безопасности в беспроводных сенсорных сетях; верификации моделей представления беспроводной сенсорной сети на предмет выполнимости условий осуществления атакующих воздействий потенциальным нарушителем; распределенных сбора, обработки и анализа больших массивов данных от программных и аппаратных сенсоров беспроводной сенсорной сети в режиме близком к режиму реального времени; выявления аномальных данных от узлов беспроводной сенсорной сети.