AON с пассивной волновой маршрутизацией

Частично обе проблемы могут быть решены на основе AON с пассивной волновой маршрутизацией. В такой сети сигнал определенной длины волны может перенаправляться (статически маршрутизироваться) в узел назначения через последовательность промежуточных узлов вместо того, чтобы широковещательно распределяться между всеми оконечными узлами сети. Это позволяет экономить энергию оптического сигнала из-за отсутствия разветвителей и допускает одновременное использование сигналов, представленных одной и той же длиной волны в разных неперекрывающихся частях сети.

AON с активной волновой маршрутизацией

Дальнейшее наращивание сети связано с переходом от статической к динамической маршрутизации. Маршрутизация на узлах становится активной и допускает дистанционное конфигурирование. Динамическая маршрутизация, прежде всего, предполагает использование оптических коммутаторов.

В. Головчук,
студентка 5 курсу факультету
Комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет;
керівник – канд. техн. наук, доц. В. В. Сергеєв

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Автоматизовані системи управління технологічними процесами (АСУ ТП) отримують все більше розповсюдження у промисловості, зв'язку, будівництві та інших сферах діяльності. У них забезпечується подальше впровадження сучасних інформаційних технологій, при цьому додаються загрози інформаційної безпеки, що є характерними для інформаційних систем. Це загрози конфіденційності, цілісності та доступності, реалізація яких може привести до значних матеріальних збитків та навіть техногенних катастроф. Прикладом цього є інцидент із центром ядерних досліджень в місті Натанз (Іран), сервер АСУ ТП якого був атакований у 2010 р. шкідливою програмою – хропаком Stuxnet. Є думка, що ця програма була створена спеціально для ушкодження АСУ ТП.

Оскільки інформаційна безпека стає актуальною для АСУ ТП, то необхідно вирішувати питання захисту інформації, яка обробляється у цих системах. Методологічною основою захисту можна вважати міжнародні стандарти у галузі інформаційної безпеки, наприклад, ISO/IEC серії 27000, а також спеціалізовані стандарти ISA (International Society of Automation) – Міжнародної Спілки Автоматизації – ANSI/ISA99.00.01-2007 і ANSI/ISA-99.02.01-2009 та ін. Рішення завдання забезпечення інформаційної безпеки АСУ ТП бачиться у комплексному поєднанні організаційних та технічних заходів захисту інформації.

Основу організаційних заходів повинна складати політика інформаційної безпеки АСУ ТП, яка повинна враховувати організацію та впровадження заходів протидії зовнішнім та внутрішнім загрозам.

Вона повинна містити, наприклад:

• визначення пріоритетних завдань щодо забезпечення цілісності, доступності або конфіденційності інформації;

• визначення основних вражливостей інформаційної складової АСУ ТП;
• визначення основних загроз безпеці інформації в АСУ ТП,
• формування моделей порушників інформаційної безпеки та виявлення мотивів їх дій;
• аналіз ризиків інформаційної безпеки та процесів керування ними;
• формування вимог до складу та архітектури системи технічних (апаратних та програмних) засобів захисту інформації;
• розробка процедур аудиту та моніторингу безпеки інформаційної складової АСУ ТП на програмному та апаратному рівнях;
• розробка комплексу організаційно-розпоряджувальної документації з питань дотримання персоналом АСУ ТП вимог інформаційної безпеки, та ін.

Як свідчить міжнародний досвід, складання політики інформаційної безпеки інформаційних систем є достатньо тривалим, складним та трудомістким процесом. Це у повній мірі відноситься і до АСУ ТП.

В. И. Гура,
кандидат технических наук, доцент,
заведующий кафедрой компьютерной инженерии,
Международный гуманитарный университет
Я. Гуревский,
студент 5 курса факультета
Компьютерных наук и инновационных технологий,
Международный гуманитарный университет

ГОРОДСКОЙ МОБИЛЬНЫЙ ИНТЕРНЕТ НА ОСНОВЕ WI-FI ПОКРЫТИЯ

В данной работе проводились исследования возможности использования Wi-Fi сетей в городских условиях для мобильного доступа к Интернету и варианты использования уже развернутых точек доступа. В наши дни большинство смартфонов и других мобильных устройств имеют поддержку Wi-Fi. Более того, ожидается значительное повышение мобильного трафика в ближайшие годы. Доступ к интернету посредством Wi-Fi это заманчивая альтернатива сотовой связи, так как это достаточно распространенная беспроводная технология, которая предоставляет высокую скорость связи и имеет низкую стоимость развертывания. В этой статье мы анализируем характеристики Wi-Fi покрытия и возможность соединения пользователей мобильных данных, используя различные скорости соединения и с различными настройками точек доступа. Эти результаты позволяют нам анализировать различные способы применения и проблемы создания городской Wi-Fi сети на основе существующей инфраструктуре основанной на уже развернутых точках доступа.

В связи с быстрым увеличением количества мобильных устройств с поддержкой доступа к Интернету, Пользователи данных устройств ожидают получения доступа к Интернету в любой точке и в любое время. По прогнозам в ближайшие годы произойдет значительный рост мобильного траффика [1]. Сотовые широковещательные сети в следствии сталкиваются с проблемами «заторов» и пропускной способности. Но усовершенствования в этих беспроводных сетях стоят дорого, а новые технологии, такие как 4G, имеют спорные результаты по производительности услуг.