Беспроводные Интернет-технологии для библиотек: постановка проблемы, примеры использования и вопросы безопасности

Wireless Internet Technologies: Problem definition, experiences and security

Бездротові Інтернет-технології для бібліотек: постановка проблеми, приклади використання і питання безпеки

Залужский С. И.
Московский государственный университет культуры и искусств, Москва, Россия

S. I. Zaluzhsky
Moscow State University of Culture and Arts, Moscow, Russia

Залужський С. І.
Московський державний університет культури та мистецтв, Москва, Росія

Рассматриваются вопросы применения мобильных технологий передачи данных в библиотеках, а также возможные проблемы безопасности в беспроводных сетях. Описаны основные способы организации безопасности в сетях при включении в них беспроводного сегмента.

The issues of using mobile technologies of data transmission in libraries, as well as the possible security problems that might arise in wireless networks, are discussed. The ways to provide network security when including wireless component are prposed.

Розглянуто питання застосування мобільних технологій передачі даних у бібліотеках, а також можливі проблеми безпеки у бездротових мережах. Описано основні способи організації безпеки у мережах при включенні до них бездротового сегменту.

Беспроводные сети привлекают внимание современного общества, которое становится все более и более мобильным прямо на наших глазах. Широкие массы пользователей только учатся тому, как просто быть все время на связи — будь это на рабочем месте, в студенческом общежитии, в кафе или дома — без применения какого-либо сетевого кабеля. Библиотеки, в свою очередь, быстро отреагировали на новые технологии и готовы в ближайшем будущем их освоить. Уже сейчас в некоторых библиотеках нашей страны и тем более за рубежом библиотекари начинают работы по предоставлению своим читателям возможности беспроводного подключения к внутренним информационным ресурсам и доступа в Интернет. Вероятно, в ближайшее время станет возможным брать напрокат ноутбуки со встроенными беспроводными модулями прямо в библиотеке.

Итак, попробуем ответить на вопрос: кому и зачем нужны беспроводные сети передачи данных?

Беспроводное оборудование используется для передачи данных на определенное расстояние. Абонентом такой сети может быть и один человек, и целая локальная сеть компании, насчитывающая сотни пользователей, - совершенно другое приложение с иными требованиями к оборудованию.

Сейчас растет количество провайдеров мобильной связи, которые предоставляют готовые решения организации беспроводного сегмента в информационной системе предприятия. В первую очередь Wi-Fi устанавливается в местах массового использования именно мобильных компьютеров и устройств, таких как аэропорты, гостиницы, отели, рестораны и кафе. Можно ожидать быстрое распространение беспроводных Интернет-сервисов в течении нескольких последующих лет. Также ожидается, что пользователи придут в библиотеки, обратятся к онлайновым справочным ресурсам, используя различные беспроводные устройства. Поэтому уже сейчас нужно готовиться и предусматривать такую возможность крупным библиотекам, а в будущем — библиотекам более мелкого масштаба.

Не смотря на то, что возможности беспроводных технологий велики, они не способны заменить традиционные проводные сети. Например, сейчас беспроводные сети имеют достаточно серьезные проблемы с точки зрения безопасности и без адекватной защиты, WLAN обеспечивают широкий, не контролируемый доступ в Интернет, что означает для хакеров легкую возможность вторжения в сеть предприятия. Помимо «хромающей» безопасности есть у беспроводных сетей, предназначенных для крупных корпоративных сред, и другой, весьма заметный недостаток — эффект «бутылочного горлышка», проявляющийся при использовании большого количества точек доступа и большого числа клиентов, подключенных к одной точке. Он выражается в виде резкого снижения пропускной способности сети, даже при условии достаточно широкого внешнего канала, соединяющего интрасеть с «внешним миром». Дело в том, что точки доступа стандартов 802.11 предоставляют разделяемую среду, в которой в данный момент времени лишь одна из них может вести передачу данных. Снижение скорости обмена информацией критично для любого пользователя, а уж

тем более для корпоративного. Как следствие, чтобы добиться эффективной работы сети, приходится прибегать к различным ухищрениям.

Однако, беспроводные сети (технологии) будучи спланированными должным образом, несомненно, применимы в библиотеках. Наше общество все больше ждет те преимущества, которые несет беспроводной доступ. Еще, крайне важен, тот факт, что беспроводные сети являются частью современных Интернет-технологий и поэтому библиотекари не должны оставаться в стороне от этого процесса.

Беспроводные технологии в библиотеках

В зарубежных университетах, которые уже сегодня довольно часто оборудованы Wi-Fi, студенты наслаждаются возможностью бродить по кампусу с ноутбуками из общежития в класс и даже в кафе, расположенном через улицу, при этом не теряя доступа в Интернет. Если институтский студгородок обеспечивает беспроводный доступ своим студентам и преподавателям, то библиотека или информационный центр не должны оставаться в стороне от этого процесса. Крайне важно для библиотек быть хорошо интегрированными в сеть большой организации, будь то проводная или беспроводная сеть. Пока спрос на беспроводные сети в библиотеках невысок, но предполагается, что рост спроса на использование данной технологии в библиотеках начнет стремительно расти уже в ближайшее время.

В дополнение к обеспечению хот-спотами (точки доступа к сети) сети беспроводного доступа в Интернет, библиотеки рассматривают и другие новаторские возможности по использованию этой технологии. Беспроводные сети могут использоваться для расширения библиотечных сервисов (услуг). Многие библиотеки предоставляют персональные компьютеры для доступа к электронному каталогу, тематическим базам данных и другим информационным ресурсам. В библиотеках довольно часты периоды пикового использования компьютеров, когда число требуемых машин превышает количество имеющихся. Увеличение количества стационарных читательских рабочих мест обычно означает: заказ компьютеров, мебели, планирования места, проводку электричества и сети. Ноутбуки с беспроводными модулями могут быть более гибким, а иногда и единственно возможным путем для расширения числа рабочих станций. Сейчас сами ноутбуки стоят ощутимо больше, чем сравнимые по мощности настольные компьютеры и пока спрос на ноутбуки будет не столь велик, хотя в нашей стране буквально со дня на день ждут валообразного увеличения спроса на ноутбуки и КПК. Ноутбуки же могут быть взяты напрокат, позволяя работать в более комфортабельных условиях, чем в перегруженных обычными компьютерами помещениях.

Wi-Fi так же может быть использован в публичных библиотеках для создания учебных лабораторий и специальных читальных залов, оснащенных ноутбуками, в которых читатели и сотрудники могут обучаться применению современных технологий. В читальных залах могут располагаться целые группы ноутбуков, укомплектованных беспроводной картой, которые могут просто перемещаться в зоне действия точки доступа. Оборудование может быть установлено в информационных центрах, школах или удаленных конференц-залах.

Сотрудники библиотеки могут использовать беспроводные сети для удаленной обработки и каталогизации заявок. Ноутбуки, укомплектованные считывателями штрих-кодов, могут использоваться для сканирования книг в комплектовании, как часть работ по каталогизации или помогать в очистке электронных каталогов.

Уязвимость беспроводных сетей

Одна из главных ловушек Wi-Fi лежит в зоне безопасности — часто говорится, что данные сети просты в применении, в тоже время, вопросы безопасности отходят обычно на второй план. Основа решения вопроса безопасности лежит в нахождении компромисса в предоставлении пользователям возможности простоты использования всех преимуществ Wi-Fi и предотвращении несанкционированных действий не авторизованных пользователей. На первом уровне вы должны знать SSID (идентификатор сессии) для получения доступа к точке доступа. Но в библиотеках часто оставляют SSID, установленный по умолчанию, это означает, что любой разбирающийся в Wi-Fi оборудовании человек может запросто получить доступ. Даже если он был изменен, SSID передается широковещательно, как часть опросного сигнала точки доступа и может быть легко расшифрован.

Первичная архитектура безопасности зависит от настройки конфигурации WEP. Если WEP отключен, пользователи могут получать доступ к сети, если они знают SSID точки доступа. Но если WEP включен, коммуникационный поток устройств, подключенных к беспроводной сети, может теоретически считаться таким же защищенным, как и на проводной сети.

WEP использует ключ безопасности для идентификации разрешенных пользователей и шифрует их трафик, который передается по воздуху. Данные шифруются ключом разрядностью от 40 до 104 бит. Но это не целый ключ, а только его статическая составляющая. Для усиления защиты применяется так называемый вектор инициализации Initialization Vector (IV). Он предназначен для рандомизации дополнительной части

ключа, что обеспечивает различные вариации шифра для разных пакетов данных. Данный вектор является 24-битным. Как не странно звучит именно динамическая часть ключа является слабым местом WEP, т.к такой ключ взламывается методом прямого подбора в течении часа. Будучи однажды взломанным, ключ будет использоваться неограниченное число раз использоваться для несанкционированного доступа. Более совершенная реализация стандарта, называемая динамический WEP,— новый ключ генерируется для каждой сессии, таким образом, обеспечивается дополнительный уровень безопасности.

Увеличение числа индивидуальных пользователей ведет к росту утечек из беспроводных сетей — не защищенный сигнал пригодный для использования распространяется далеко за пределы своей целевой аудитории. Имеется большое количество технических средств для вторжения в организацию беспроводной сети. Направленная антенна стоит порядка 60$, она выводит сигналы точки доступа далеко за пределы ожидаемого диапазона действия — например, парковки возле здания. Лишь однажды подключившись, можно сколько угодно использовать открытые, уязвимые сетевые сервисы. Взлом беспроводных сетей перерос, можно сказать, в хакерский спорт, часто называемый «war driving» дословно «военное движение».

Существенное улучшение безопасности в беспроводных сетях может принести применение WPA (стандарт безопасности) и VPN (технология виртуальных частных сетей). WPA это временный стандарт до вступления в силу IEEE 802.11i, технология защищенного доступа к беспроводным сетям(Wi-Fi protected access). Ключевыми модулями здесь являются TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol) и MIC — технология проверки целостности сообщений (Message Integrity Check). Стандарт TKIP использует автоматически подобранные 128-битные ключи, общее число вариации таких ключей 500млрд. Внешнему проникновению и изменению информации в сети препятствует и технология проверки целостности сообщений MSI. Достаточно сложный математический алгоритм позволяет сверять данные, отправленные в одной точке и принятые в другой.

Хотя безопасность в Wi-Fi технологиях будет и далее улучшаться, эти сети требуют крайней осторожности при работе с ними. Беспроводные сети должны быть очень тщательно и отчетливо отделены от корпоративной сети библиотеки. VLANS или файерволы могут гарантировать, что даже в случае несанкционированного доступа, пользователь не сможет получить более чем просто свободный доступ в Интернет. А иногда даже такую возможность системный администратор может закрыть.

В заключение хотелось бы отметить, что рассмотренные возможности применения беспроводных Интернет-технологий открывают новые горизонты в развитии библиотечно-информационных систем.