ОСОБЕННОСТИ БЕСПРОВОДНОЙ СВЯЗИ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ УГРОЗ ДЛЯ БЕЗПРОВОДНОЙ СЕТИ

А.К. Курманбай, студент гр. 17В41
Научный руководитель: Разумников С.В. ассистент
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail: aigera_0796@mail.ru

Как и множество других инновационных технологий, беспроводные сети сулят не только новые выгоды, но и риски. Бум Wi-Fi породил целое поколение хакеров, специализирующихся на изобретении новых способов взлома корпоративных инфраструктур и атак пользователей.

Особенности беспроводной связи с точки зрения безопасности. Традиционные проводные сети используют для передачи данных кабель, который считается «контролируемой» средой, защищенной зданиями и помещениями, где он проложен. Внешний трафик, входящий в защищенный сегмент сети, фильтруется брандмауэром и анализируется системами IDS/IPS. Для того чтобы получить доступ к такому сегменту проводной сети, злоумышленнику необходимо преодолеть либо систему физической безопасности здания, либо брандмауэр.В случае же беспроводных сетей используется открытая среда с практически полным отсутствием контроля. Обеспечить эквивалент физической безопасности проводных сетей здесь просто невозможно. Беспроводной сегмент сети становится доступным с другого этажа или снаружи: единственной физической границей беспроводной сети является уровень самого сигнала. Поэтому, в отличие от проводных сетей, где точка подключения пользователя известна, к беспроводным подсоединиться можно откуда угодно, лишь бы сигнал был достаточной мощности. При этом приемник, работающий только на прослушивание, вообще невозможно определить.

Еще большую проблему создает то, что беспроводные пользователи по определению мобильны. Они могут появляться и исчезать, менять свое местоположение и не привязаны к фиксированным точкам входа. Главное – находиться в зоне покрытия. Все это значительно осложняет задачу отслеживания.

Следующую проблему обеспечения беспроводной безопасности, на этот раз – пользователя, представляет такая важная составляющая мобильности, как роуминг. С помощью специального ПО его достаточно несложно «пересадить» с авторизованной точки доступа на неавторизованную или даже на ноутбук злоумышленника, работающий в режиме Soft AP (программно реализованной точки доступа). Это открывает возможность для целого ряда атак на ничего не подозревающего пользователя.

Риски беспроводной сети, беспроводные технологии, работающие без физических и логических ограничений своих проводных аналогов, подвергают сетевую инфраструктуру и пользователей значительным рискам. Для того чтобы понять, как обеспечить безопасное функционирование беспроводных сетей, давайте рассмотрим их подробнее.

Развитием информационных технологий играет большую роль в жизни человека.

Интернет стал неотъемлемой частью нашей жизни, так как он пользуется нами повседневно: проверяя почту, сидя в социальных сетях, общаясь в социальных сетях, просматривая фильмы и видео. И зачастую использование проводного интернета является нецелесообразным, так как он ограничивает наше перемещение, а провода путаются и мешаются.

Подробнее расмотрим wi-fi и безопасность при работе. Так как замену проводам пришли Wi-Fi технологии, которые позволили, подключаться к высокоскоростному Интернету не используя проводные соединения. Wi-Fi получил широкое распространение при организации беспроводного интернета во многих современных предприятиях, школах, домах, университетах и в публичных местах, как альтернатива проводному интернету. Большинство современных портативных устройств (ноутбуки, КПК, смартфоны) имеют встроенные средства для работы в беспроводных сетях. Количество точек беспроводного доступа в мире растет с каждым днем, и при этом мы можем выйти в интернет, откуда угодно и без особых проблем. Самое главное, чтобы под рукой оказался ноутбук, смартфон или планшетный компьютер[1]. Находясь в кафе, торговом комплексе, дома или на работе мы используем Wi-Fi сети, так как это удобно, практично и мобильно. Но немногие задавались вопросом, безопасно ли это?

Wi-Fi или Wireless Fidelity переводится как «высокая точность беспроводной передачи данных». Это стандарт оборудования для построения локальных вычислительных сетей. В сети, созданной по технологии Wi-Fi, передача данных осуществляется без физического соединения устройств, посредством радиосигнала. Еще одним неоспоримым преимуществом (кроме отсутствующих прово-

дов) является простота развертывания и настройки Wi-Fi и при этом одна точка доступа может обеспечить охват в радиусе до 200 метров, в зависимости от роутера. Широкое распространение, помимо домашних и офисных сетей, Wi-Fi нашел в сфере организации публичного доступа в Интернет (хотспотов). Стандарт IEEE802.11n – один из передовых стандартов Wi-Fi, на данный момент. Используются частотные каналы в спектрах 2.4GHz и 5GHz. Совместим с 11b/11a/11g. Стандарт 802.11n использует совершенно новые технологии, повышающие скорость передачи данных и увеличивающие радиус покрытия. Так, например, заявленная скорость передачи данных для этого стандарта – около 430Мбит\с. Используется модуляция – MIMO (Multiple Input Multiple Output). Данная модуляция построена на основе применения множества антенн, соответственно, создается множество информационных потоков, что в разы увеличивает скорость передачи данных [2].

Для удобства передачи данных частота поделена на так называемые каналы.

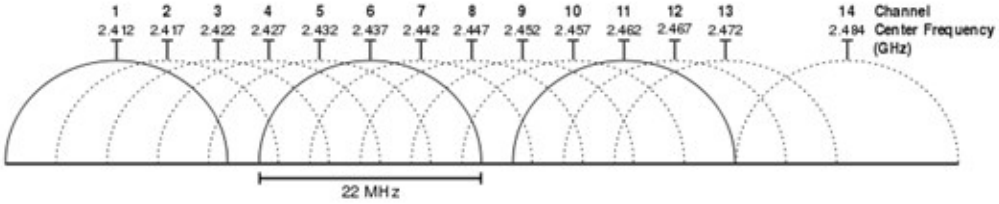

Рис. 1. Распределение частот по каналам

Из изображения видно, что каналов всего 14, но в зависимости от страны, в которой мы находимся, разрешенными для использования могут быть только некоторые из них. Так, например, в России разрешено использовать с 1 по 13 канал в США с 1 по 11, а в Японии все 14.

При передаче данных по сети немаловажным аспектом является шифрование трафика, так как для перехвата передаваемой информации не нужно физическое воздействие, а достаточно просто подключиться к сети и, «подслушивая» канал, перехватывать информацию. На данный момент существуют несколько видов шифрования, таких как:

1. WEP. Самый простой алгоритм шифрования. Поддерживается всеми точками доступа и клиентами.

2. WPA. В основе используется все тот же RC4, но дополнительно применяются алгоритмы TKIP и MIC.

Суть алгоритма — проверка целостности данных, чтобы исключить возможность подделки пакетов. Протокол WPA так же поддерживается всеми устройствами без проблем в его двух вариантах:

WPA-PSK — здесь используется заранее предопределенная ключевая фраза в качестве пароля. Этот вариант часть применяется в домашних условиях.

WPA-802.1x — доступ к сети осуществляется после проверки дополнительным сервером аутентификации. Этот способ наиболее подходит для крупных организаций. Из этих двух вариантов легче всего взломать WPA-PSK, однако это будет все равно тяжелее, чем WEP.

С целью обеспечения большей надежности защиты информации был разработан стандарт WPA2.

WPA2 Основное отличие от WPA заключается в использовании более стойкого алгоритма шифрования AES [1].

Технология Wi-Fi безусловно удобна и универсальна для организации беспроводного доступа к информации. Однако она несёт в себе множество серьёзных угроз информационной безопасности. Wi-Fi-соединение может быть взломано, а данные перехвачены посредством сниффинга («прослушивания» сетевого трафика) либо атак по типу man-in-the-middle attack (MITM). Этот способ является наиболее простым, так как не нужно физическое воздействие.

Вопрос безопасности wi-fi сетей актуален, так как сниффинг программы находятся в открытом доступе и на основе данных программ можно показать наглядно, как небезопасны беспроводные сети в независимости от сложности пароля и шифрования трафика.

Алгоритм перехвата выглядеть следующим образом:

Пользователь, идентифицировавшийся в сети, как правило, отправляет данные на беспроводной маршрутизатор. Эту информацию в дальнейшем можно перехватить и прочитать, но не ту, что зашифрована, например пароль от почты или логин. Для того чтобы после каждого клика пользователь не вводил пароль, сайт посылает ему «идентификатор сессии» после входа в систему, который

нужен для работы с сайтом, которые хранятся в «куки». Для защищенных WPA/WPA2 Wi-Fi-сетей программа использует DNS-Spoofing атаки. ARP-Spoofing означает, что она заставляет все устройства в сети думать, что программа — виртуальный роутер, и пропускает все данные через себя. Благодаря чему зашифрованная информация перехватывается, и злоумышленник получает доступ к вашей информации: почте, социальным сетям, запросам в поисковиках и других посещённых сайты. Таким образом, сниффинг является одной из актуальных проблем в Wi-Fi сетях. И для того, чтобы обезопасить себя в беспроводных сетях, необходимо:

При подключении к сети устанавливать зашифрованное соединение HTTPS-протокол и SSL.

После каждого подключения к открытым сетям менять пароль или использовать антисниффинг программы заблаговременно проанализировав перед отправкой своих данных по сети.

Литература.

1. Щербяков, А. К. Wi-fi: всё, что вы хотели знать, но боялись спросить/ А. К. Щербяков. — М.: Бук-пресс, 2005–11 с.
2. Постановление Правительства Российской Федерации от 12 октября 2004 г. № 539 г.
3. Курманбай А. К. Угрозы безопасности информации при работе с WI-FI [Электронный ресурс] // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов II Международной конференци, Томск, 19-22 Мая 2015. - Томск: ТПУ, 2015 - С. 811-813. - Режим доступа: http://www.lib.tpu.ru/fulltext/c/2015/C24/C24.pdf

РОЛЬ СИСТЕМНО-ДИАГНОСТИЧЕСКОГО АНАЛИЗА В ЭКОНОМИКЕ

С.В. Кучерявенко, к.филос.н., доц., А.В. Горбатова, студ.*
ГБОУ СПО Юргинский технологический колледж
652050, г. Юрга, ул. Заводская, 14, тел. (838451) 5-37-00
E-mail: serg_kuch60@mail.ru
**Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета*
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел. (838451) 5-44-32
E-mail: avgorbatova@tpu.ru

Состояние современной мировой и отечественной экономики характеризуется возрастающими динамизмом, многообразием и неопределённостью происходящих в ней изменений. Как показывает экономическая практика, растущие потоки информации требуют как соответствующей реакции, так и умения оперативного принятия решений. Макроэкономические параметры, которые должны устанавливаться и регулироваться соответствующими государственными структурами (Правительство, Центральный банк и пр.) в последнее время часто оказываются неадекватными складывающейся в отечественной и мировой экономике ситуации. Причём мы наблюдаем расширяющееся расхождения мнений различных учёных экономических сообществ относительно постановки диагноза и выбора путей выхода из затянувшегося системного кризиса. Подобное «лечится» подобным – главный принцип медицины. Системный кризис требует системного же анализа. Вот почему столь актуальна разработка специфической методологии познания сверхсложных социально-экономических систем, которая легла бы в основу создания современных технологий управления. Такой методологией является системно-диагностический анализ [1].

Диагностика реального состояния объекта вкупе с характеристикой и детерминантами происходящих в нём глубинных изменений всегда была и остаётся актуальной в различных сферах человеческой деятельности. Понятно, что любая из областей осуществления диагностики, а, значит, и соответствующая диагностика имеет собственную характерную специфику. Однако диагностированию присущи также всеобщие черты и закономерности, обусловленные, с одной стороны, атрибутивностью диагноза для любой целенаправленной деятельности, с другой – системной природой диагностируемых объектов. А главное, точный диагноз –необходимая предпосылка адекватного прогнозирования, проектирования, моделирования и прочих аспектов социально-экономического регулирования на всех уровнях социума.

С точки зрения марксистской социальной философии, базисом общества является экономика. Об этом рассуждал ещё Аристотель – «первопроходец» экономического диагноза (учение об «ойкономике» и «хрематистике» и основных «симптомах»-признаках отнесения хозяйства соответственно к продуктивному либо бесплодному). Всё дальнейшее развитие экономической теории так или иначе