УДК 004.056.53

С. С. Старцев

Новосибирский государственный
архитектурно-строительный университет (Сибстрин)
ул. Ленинградская, 113, Новосибирск, 630008, Россия
E-mail: helionthefirst@gmail.com

К ВОПРОСУ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ НА БАЗЕ ТЕХНОЛОГИИ WI-FI [*]

В статье описана проблема безопасности сетей, построенных с использованием устройств беспроводной передачи данных, коротко представлены преимущества данной технологии и недостатки в плане обеспечения надлежащего уровня безопасности. Представлена методика, оценивающая уровень защищенности Wi-Fi точек доступа в автоматическом режиме, и дан краткий обзор собранной статистической информации.

Ключевые слова: информационная безопасность, сетевые технологии, беспроводные устройства, тест на проникновение.

Введение

Уровню обеспечения безопасности беспроводных устройств уделяется в настоящее время крайне малое внимание. Но этот показатель в свою очередь является очень важной характеристикой общего уровня информационной безопасности сетей. Многие из существующих алгоритмов шифрования и аутентификации имеют уязвимости, позволяющие подключиться к беспроводному устройству неавторизованному пользователю либо получить полный контроль над данным устройством. В настоящее время анализ уровня защиты беспроводных устройств на базе технологии Wi-Fi производится только при проведении полного внутреннего аудита информационной безопасности организации и подразумевает априорное знание используемых протоколов и технологий. Но для массового анализа и сбора статистической информации такой метод не подходит. Требуется реализовать методику и работающий прототип системы, производящей сбор статистической информации в максимально автоматизированном режиме, и постараться достоверно оценить уровень безопасности каждого устройства с помощью методики на основе экспертной оценки.

Аспекты безопасности беспроводных сетей на базе технологии Wi-Fi

Одной из широко используемых технологий беспроводной передачи данных является технология Wi-Fi (Wireless Fidelity). Это современная беспроводная технология соединения компьютеров в локальную сеть WLAN (Wireless Local Area Network).

Беспроводные сети развертываются во многих общественных местах (для создания эффективной информационной инфраструктуры предприятия, для создания канала передачи информации), где другие варианты невозможны по ряду причин или являются слишком дорогими в реализации. К середине первого десятилетия XXI в. счет количества пользователей данной беспроводной технологии передачи информации пошел на десятки миллионов. Это

[*] Автор выражает благодарность руководителю академической программы ЗАО «Лаборатория Касперского» в Новосибирском государственном архитектурно-строительном университет (Сибстрин) И. В. Ершову за постоянное внимание к работе и обсуждение ее результатов.

обусловлено рядом неоспоримых преимуществ по сравнению с классическими кабельными сетями:

1) возможность перемещения подключенного устройства в рамках зоны покрытия без потери сигнала;

2) достаточная скорость (до 600 Мб/с) передачи информации для выполнения большого спектра задач;

3) развертывание беспроводной сети может быть единственным доступным решением, если прокладка кабельного соединения между узлами сети невозможна;

4) доступность (низкая стоимость развертывания) для использования при построении небольшой домашней или корпоративной локальной сети.

Но с данными плюсами технологии тесно граничат и ее минусы, одним из основных является большое количество возможностей для неавторизованного доступа и проникновения в закрытый сегмент корпоративной сети. Здесь и далее речь будет идти именно об анализе защищенности беспроводных сетей. Данные методики анализа одинаково применимы к исследованию домашних беспроводных сетей, публичных сетей в общественных местах или закрытых корпоративных сетей.

Получение доступа к внутрисетевым ресурсам изолированной кабельной сети возможно только при наличии физического доступа к одному из сетевых устройств, входящих в целевую сеть, либо к самим каналам связи.

При использовании беспроводных сетей данное условие не является обязательным. Для попытки получения неавторизованного доступа достаточно находиться в зоне действия сигнала беспроводной сети. Злоумышленника в данном случае существенно сложнее обнаружить и даже просто заметить его присутствие, так как он может находиться в режиме пассивного прослушивания сетевого трафика.

Анализ уровня защищенности беспроводных сетей может производиться двумя способами: внутренним и внешним. Внутренний анализ подразумевает знание топологии сети, используемого оборудования, методов шифрования и аутентификации. В данной работе будет рассматриваться анализ уровня защиты без априорного знания свойств сети, т. е. внешним методом. Созданные скрипты и программное обеспечение в автоматическом режиме выполняют анализ точек доступа (Access Point), оценивают качество защищенности и представляют рекомендации для улучшения уровня надежности.

Оценка параметров защищенности беспроводных сетей

Для сканирования эфира и определения настроек сетевых устройств использовалась консольная утилита iwlist, входящая по умолчанию в большинство дистрибутивов операционных систем семейства Linux. В нашем случае, для тестирования написанных скриптов и программного обеспечения в большей мере использовалась операционная система Ubuntu 9.04.

В процессе сканирования беспроводной сети имеется возможность определить значения следующих параметров точки доступа:

1) ESSID;
2) MAC-адрес;
3) скорость передачи данных;
4) частота передачи данных;
5) номер канала передачи данных;
6) уровень сигнала, уровень шума;
7) режим работы сетевой карты устройства;
8) наличие шифрования;
9) метод шифрования;
10) протокол группового шифрования (Group Cipher);
11) протокол парного шифрования (Pairwise Cipher);
12) способ аутентификации.

Рассмотрим некоторые ключевые параметры, которые оказывают влияние на уровень защищенности беспроводной Wi-Fi сети, более подробно.

ESSID – идентификатор беспроводной локальной сети. ESSID может быть доступным для сканирующего, а может быть скрыт при конфигурировании Wi-Fi устройства. Отсутствие знания идентификатора сети не влияет прямым образом на уровень безопасности, но отображение идентификатора потенциально может дать злоумышленнику дополнительную информацию о топологии корпоративной сети или о наименовании производителя оборудования при использовании стандартного идентификатора.

Режим работы сетевой карты устройства. В стандарте 802.11 определены два способа организации сети: инфраструктурный (Infrastructure) и независимый (Independent), часто также называемый одноранговым (Ad-Hoc). В инфраструктурном режиме функции координации передачи данных выполняет точка доступа. Беспроводные станции пользователей через нее взаимодействуют друг с другом. В одноранговой сети точка доступа отсутствует, все станции являются равноправными членами системы и общаются между собой напрямую.

Возможные режимы работы сетевой карты [1].

1. Ad-Hoc – работа сетевой карты в одноранговой сети.
2. Master – работа сетевой карты в режиме точки доступа при инфраструктурном способе организации сети.
3. Managed – работа сетевой карты в режиме клиентского устройства.
4. Monitor – режим сетевой карты, при котором устройство не подключено ни к одной сети, но при этом прослушивает трафик.
5. Repeater – работа устройства в качестве повторителя между другими устройствами, находящимися друг от друга на большом расстоянии.
6. Secondary – устройство включается в работу сети только при выходе из строя другого, для которого он является «запасным».

Можно сделать вывод, что устройством, к которому физически может подключиться злоумышленник, может быть только устройство, работающее в режиме Master и Ad-Hoc.

Теоретически режим Ad-Hoc является более защищенным в сравнении с Master, так как большая часть программного обеспечения, целью которого является вторжение в целевую закрытую беспроводную сеть, ориентировано на работу с устройствами, функционирующими в режиме Master.

Наличие шифрования передаваемого трафика является ключевым параметром в безопасности беспроводной сети. Перечисленные ниже параметры могут быть определены при наличии шифрования.

Метод шифрования определяет метод шифрования данных согласно стандарту.

С помощью протокола парного шифрования шифруются и расшифровываются одноадресные фреймы, которые предназначены для единственного пользователя.

Протокол группового шифрования используется для шифрования широковещательных или многоадресных фреймов.

Способ аутентификации обозначает способ аутентификации, использующийся в сети при наличии шифрования.

Окончательный список определяемых при сканировании параметров, которые влияют на безопасность беспроводной сети и будут учитываться при расчете оценки защищенности точки доступа Wi-Fi, представлен в табл. 1.

Для ранжирования значений параметров точки доступа использовался метод экспертной оценки.

В качестве экспертов выступали: Виталий Александрович Камлюк (руководитель российского исследовательского центра ЗАО «Лаборатория Касперского»), Олег Алексеевич Ишанов (руководитель группы инфраструктурных исследований ЗАО «Лаборатория Касперского»), Денис Игоревич Масленников (руководитель группы исследования мобильных угроз ЗАО «Лаборатория Касперского»), а также сотрудники Центра финансовых технологий (ЦФТ).

В данном случае оценка каждого из значений параметров производилась независимо от совокупности имеющихся средств защиты. Каждое значение параметра оценивалось в баллах от 0 до 100 в зависимости от уровня защиты точки доступа в целом, обеспечиваемого данным средством (табл. 2).

Таблица 1

Возможные значения определяемых параметров

ESSID	Any	Открытый ESSID
	Off	Скрытый ESSID
Режим работы сетевой карты	Master	Точка доступа (режим инфраструктурный)
	Ad-Hoc	Режим Ad-Hoc
Наличие шифрования	Off	Шифрование не используется
	On	Шифрование используется
Метод шифрования	WEP	Wired Equivalent Privacy
	WPA	Wi-Fi Protected Access
	WPA2	Стандарт IEEE 802.11i
Групповое шифрование	WEP 40	WEP-шифрование, ключ 40 бит
	WEP 104	WEP-шифрование, ключ 104 бита
	TKIP	Temporal Key Integrity Protocol
	CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
	WRAP	Wireless *Robust* Authenticated Protocol
Парное шифрование	WEP 40	WEP-шифрование, ключ 40 бит
	WEP 104	WEP-шифрование, ключ 104 бита
	TKIP	Temporal Key Integrity Protocol
	CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
	WRAP	Wireless *Robust* Authenticated Protocol
Способ аутентификации	PSK	Аутентификация с общим ключом (Pre-Shared Key)
	802.1x	Аутентификация по протоколу 802.1x

Таблица 2

Результаты экспертных оценок

№	Параметр	Значение	Эксперт			
			1	2	3	4
1	ESSID	Any	0	0	0	0
		Off	10	5	5	6
2	Режим работы сетевой карты	Master	0	0	0	0
		Ad-Hoc	15	5	10	10
3	Метод шифрования	Отсутствие шифрования	0	0	0	0
		WEP	5	10	10	8
		WPA	40	40	40	40
		WPA2	60	50	60	56
4	Групповое шифрование	Отсутствие шифрования	0	0	0	0
		WEP 40	4	5	10	6
		WEP 104	5	7	30	14
		TKIP	40	15	55	36
		CCMP	70	20	65	51
		WRAP	75	20	75	56

Окончание табл. 2

№	Параметр	Значение	Эксперт			
			1	2	3	4
5	Парное шифрование	Отсутствие шифрования	0	0	0	0
		WEP 40	4	5	10	6
		WEP 104	5	7	30	14
		TKIP	40	15	55	36
		CCMP	70	20	65	51
		WRAP	75	20	75	56
6	Способ аутентификации	Отсутствие аутентификации	0	0	0	0
		PSK	30	10	30	23
		802.1X	60	30	40	43

Таблица 3

Оценки параметров по 100-балльной шкале

№	Параметр	Значение	Оценка
1	ESSID	Any	0
		Off	2,9
2	Режим работы сетевой карты	Master	0
		Ad-Hoc	4,3
3	Метод шифрования	Отсутствие	0
		WEP	3,6
		WPA	17,4
		WPA2	24,6
4	Групповое шифрование	Отсутствие	0
		WEP 40	2,7
		WEP 104	6
		TKIP	15,9
		CCMP	22,4
		WRAP	24,6
5	Парное шифрование	Отсутствие	0
		WEP 40	2,7
		WEP 104	6
		TKIP	15,9
		CCMP	22,4
		WRAP	24,6
6	Аутентификация	Отсутствие	0
		PSK	10,1
		802.1X	18,8

В табл. 3 приводятся нормированные оценки параметров защищенности на основе мнений экспертов. В рамках данной статьи описание методики нормирования не приводится.

Форматы данных и используемое оборудование

В процессе разработки, тестирования и использования написанного программного обеспечения в большей мере использовались два ноутбука со следующими конфигурациями оборудования и операционных систем:

- Packard Bell EasyNote BG46: dual-core T2390 1,86 ГГц, 1 ГБ DDR2, WiFi WLAN AW-GE780VD 802.11BG. Операционная система – Ubuntu 9.04;
- Acer 4310: Intel Celeron 1.6ГГц, 1 ГБ DDR2, WiFi Intel® PRO/Wireless 3945ABG. Операционная система – Arch Linux.

Выбор операционной системы семейства Linux был обоснован наличием для нее необходимых утилит и программного обеспечения, позволяющего производить анализ защищенности беспроводных сетей и компьютерных систем, а также дающего возможности проведения пентестинга [1] целевых объектов.

```
wlan0     Scan completed :
          Cell 01 - Address: 00:1E:58:81:6B:99
                    ESSID:"relkwifi"
                    Mode:Master
                    Channel:6
                    Frequency:2.437 GHz (Channel 6)
                    Quality=67/100  Signal level:-59 dBm  Noise level=-102 dBm
                    Encryption key:on
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (1) : TKIP
                        Authentication Suites (1) : PSK
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                              9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s
                              48 Mb/s; 54 Mb/s
                    Extra:tsf=0000000019708181
                    Extra: Last beacon: 20ms ago
          Cell 02 - Address: 00:1E:4A:9A:01:10
                    ESSID:"ssidjh1"
                    Mode:Master
                    Channel:5
                    Frequency:2.432 GHz (Channel 5)
                    Quality=21/100  Signal level:-89 dBm  Noise level=-103 dBm
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s
                              48 Mb/s; 54 Mb/s
                    Extra:tsf=0000000ddb61b181
                    Extra: Last beacon: 7216ms ago
```

Рис. 1. Результат выполнения утилиты iwlist scan

Для получения информации о беспроводных сетях используется утилита *iwlist* (рис. 1), которая выводит необходимую информацию для внешнего анализа уровня защищенности.

[1] Pentesting – тестирование на проникновение, попытка внешнего проникновения в закрытую сеть или целевую компьютерную систему с целью выявления ее уязвимостей, с последующим описанием рекомендаций по их устранению.

Программная реализация методики оценки защищенности

Оценка уровня безопасности беспроводных сетей производится с приведением итоговых баллов к 100-балльной системе. Чем больше количество набранных баллов, тем надежнее беспроводное взаимодействие устройств внутри данной сети.

Первоначальная реализация программного обеспечения была написана с использованием библиотеки Qt4 на языке C++. Программа умела производить поиск беспроводных устройств, рассчитывать баллы уровня защищенности и выводить полученные данные в консоль пользователю либо в диалоговое окно, при запуске ПО с графическим интерфейсом (рис. 2).

```
relk@relk-laptop:~/Документы$ sudo ./sc

Berkaev --> 54.5
ssidjh1 --> 50.6
relkwifi --> 50.6
dlink-ntk266 --> 63.9
Pasha --> 22.0
Segmentation fault
relk@relk-laptop:~/Документы$
```

Рис. 2. Отображение рассчитанных баллов в консоль пользователя

Но для полноценной массовой и автоматизированной обработки полученных данных этого оказалось недостаточно. Необходимо было собрать большое количество информация о параметрах точек доступа, которая нужна для представительной статистической обработки и общего отражения состояний безопасности беспроводных устройств Новосибирска, а также о распространенности использования сетевых устройств в разных районах города. В программной реализации возникла необходимость иметь следующие функциональные возможности.

1. Возможность сбора информации в автоматическом режиме с наименьшим участием пользователя.
2. Реализация алгоритма расчета баллов уровня защищенности.
3. Реализация алгоритма расчета уровня достоверности оценки.
4. Построение актуальных статистических графиков и возможность их использования в сторонних материалах.
5. Сохранение метаданных, таких как время проведения сканирования, полный текст вывода утилиты iwlist.
6. Привязка процесса сканирования к районам города.
7. Возможность обмена собранной информацией между различными пользовательскими машинами (импорт / экспорт собранной информации с учетом возможности появления дублирующейся информации).

Для реализации данного функционала программная реализация была переписана с использованием Apache, PHP, MySQL и Bash. Процесс сбора статистической информации сводится к перемещению со сканирующим компьютером по различным районам города. Через установленные интервалы времени производится сканирование эфира на предмет обнаружения беспроводных устройств, работающих с использованием технологии Wi-Fi, и сохранение в базу данных информации о точках доступа и их конфигурации, если данные по текущей точке доступа ранее не сохранялись.

После разбора и сохранения производится оценка каждой точки доступа согласно описанной выше методике с учетом актуальных экспертных данных. После этого информация визуализируется в виде графиков.

Статистика

При проведении тестирования написанного программного обеспечения было произведено агрегирование информации о 2 117 точках доступа. Информация о количестве точек доступа, обнаруженных при сканировании (производилось во время движения на автомобиле при помощи стандартных Wi-Fi адаптеров, встроенных в ноутбук, без использования дополнительных антенн или других устройств для лучшего приема / передачи сигнала) всех районов города, представлена на рис. 3.

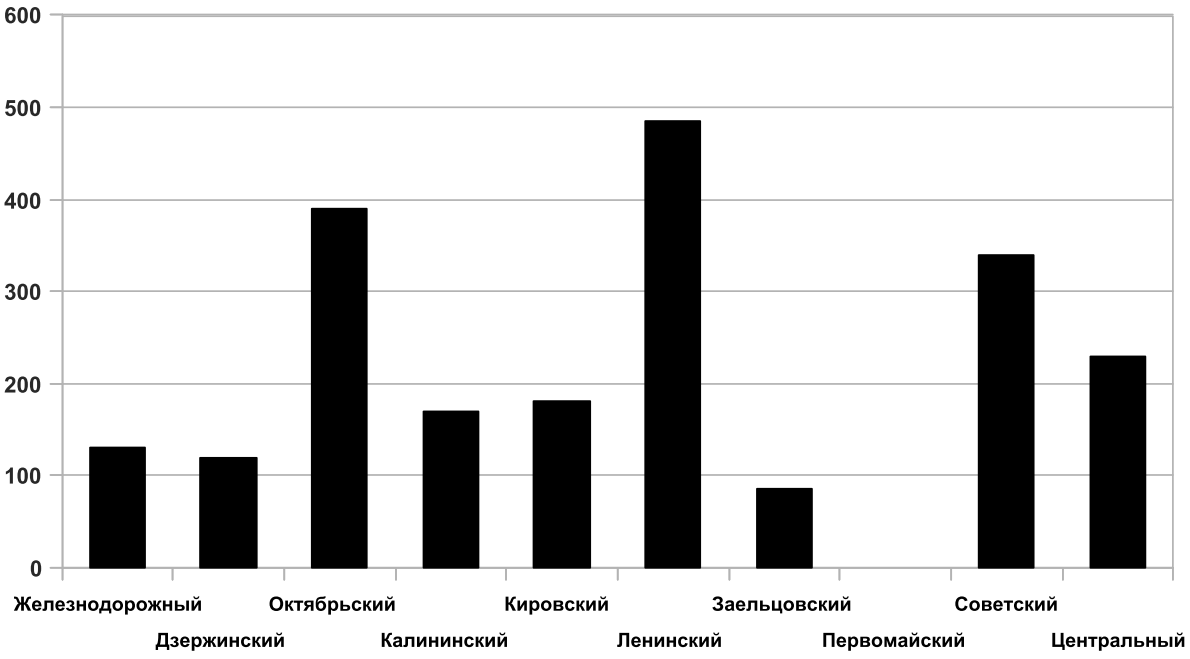

Рис. 3. Количество обнаруженных точек доступа по районам города

Количество обнаруженных точек доступа в ряде районов больше, чем в остальных. Это объясняется наличием в этих районах крупных жилых застроек (микрорайонов).

Несмотря на то что беспроводные точки доступа активно используются частными лицами, у данного класса устройств (бюджетные со стандартным набором функциональных возможностей) недостаточно мощный передатчик, чтобы транслировать сигнал на необходимое расстояние и быть обнаруженным с дорог общественного пользования или междворовых проездов. Выпадение из общей картины Первомайского района можно объяснить нахождением на территории данного района разрозненных жилых домов и практически полным отсутствием коммерческих организаций.

На рис. 4 отражен средний уровень безопасности точек доступа, находящихся на территории каждого из районов. По вертикальной оси отложено среднее значение баллов защищенности внутри данного района города.

Средний уровень защищенности с группировкой по районам находится в диапазоне между 34,11 и 46,8 балла по оценочной 100-балльной шкале. На данные величины оказывают достаточно сильное влияние беспроводные точки доступа, которые введены в эксплуатацию без дополнительной настройки и конфигурирования, т. е. «из коробки». Это еще раз подтверждается тем, что среди обнаруженных устройств достаточно много устройств со стандартными идентификаторами ESSID, установленными по умолчанию производителем устройства.

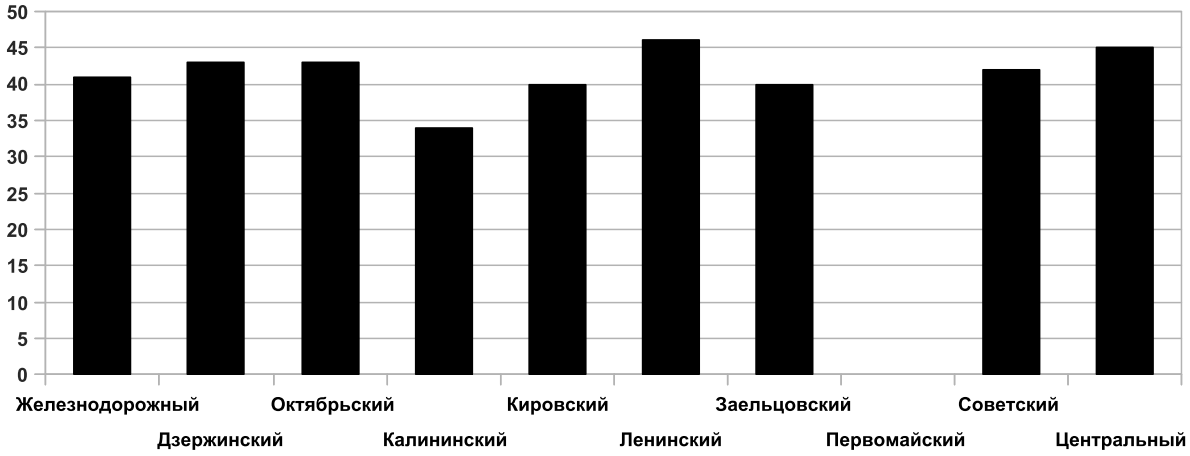

Рис. 4. Средний уровень защищенности по районам города

Данной методикой можно производить массовый анализ уровня защищенности точек доступа, но для более подробного и точного анализа необходимо производить дополнительные оценочные действия для анализа каждого конкретного устройства беспроводной связи.

Рекомендации обеспечения безопасности беспроводных устройств

Приведем несколько правил (доступных пользователю, не обладающему глубокими знаниями администрирования сетевых устройств), помогающих выполнить настройку Wi-Fi точки доступа либо маршрутизатора, чтобы максимально обезопасить передаваемую в сети информацию.

1. Если функциональные возможности точки доступа позволяют запретить ее настройку, используя соединение по радиоканалу, – запретите. Для настройки такой точки доступа будет возможность подсоединения с помощью проводного интерфейса, а у злоумышленника такой возможности не будет.
2. По возможности используйте алгоритм шифрования WPA2, алгоритм WEP является морально устаревшим.
3. Не используйте в названии точки доступа (ESSID) наименование, позволяющее идентифицировать ее принадлежность к конкретному владельцу или организации. Избегайте названий, содержащих наименования фирмы изготовителя и модели устройства. Желательно запретить вещание ESSID неавторизованным клиентам.
4. IP-адреса на клиентских компьютерах сети устанавливайте вручную, не используйте без необходимости DHCP, так как использование данной технологии облегчает злоумышленнику соединение, после того как он узнал / взломал ключ доступа.
5. Если точка доступа позволяет включить фильтрацию по MAC-адресам, включите ее и добавьте адреса предполагаемых клиентских машин.
6. Используйте длинные ключи доступа, состоящие из различных символов, букв и цифр.

В перспективе данной работы планируется реализация следующих функциональных возможностей написанного программного обеспечения.

1. Возможность изменения оценочных шкал, т. е. добавление оценок новых экспертов и корректировка итоговых баллов по каждому параметру с учетом новых экспертных данных.
2. Отображение рекомендаций по каждой точке доступа, следуя которым можно сделать передачу информации по беспроводной сети более безопасной.

Безопасность беспроводных сегментов сетей – достаточно важная часть информационной безопасности, которой необходимо уделять достаточное внимание. Из-за несовершенства средств обеспечения безопасности беспроводных устройств к вопросу использования данной

технологии передачи информации в сетях (особенно корпоративных, с критически-важной информацией) стоит подходить с особым вниманием.

Заключение

Представленная в статье методика оценки уровня безопасности беспроводных устройств на базе технологии Wi-Fi позволяет использовать ее без доступа к внутренней сетевой архитектуре и достаточно хорошо анализирует как корпоративные точки доступа, так и домашние частные точки доступа. Реализован работающий прототип системы сбора информации о беспроводных устройствах в максимально автоматизированном режиме, производящий оценивание уровня безопасности по приведенной 100-балльной шкале, а также визуализирующий полученную обработанную информацию в виде наглядных графиков. Обработка статистической информации по беспроводным устройствам Новосибирска показала, что большое их количество используют настройки по умолчанию, т. е. те же ESSID и протоколы шифрования и аутентификации, которые были установлены при производстве. Из этого можно сделать два вывода: во-первых, о недостаточной компьютерной грамотности пользователей, использующих данные устройства, что не позволяет произвести настройку, соответствующую современным требованиям обеспечения безопасности. Во-вторых, пользователи тем самым не осознают, что вся информация, передающаяся по плохо защищенным каналам связи, может быть украдена и использована злоумышленниками. Среди передаваемой информации могут оказаться, кроме частной информации (фотографии, видеофайлы, документы), логины и пароли к почтовым и другим сервисам. Приведенные рекомендации позволяют настроить беспроводное устройство для обеспечения достаточного уровня безопасности. Данные рекомендации доступны для пользователей, не обладающих глубокими знаниями в области администрирования сетей.

Список литературы

1. *Владимиров А. А.* Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей. М.: НТ Пресс, 2005. 463 с.

Материал поступил в редколлегию 05.10.2011

S. S. Startsev

LEVEL SECURITY OF WIRELESS NETWORK BASED ON WI-FI TECHNOLOGIES

This article describes the problem of network security, built with the use of devices for wireless data transmission, briefly presented the advantages and disadvantages of this technology in terms of providing an adequate level of security of such networks. Submitted by the method estimating the level of security Wi-Fi access points in the automatic mode, and given a short overview of the collected statistical information.

Keywords: information security, network technologies, wireless devices, antivirus technologies, penetration testing.