

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ
И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ИССЛЕДОВАНИЕ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ
СТАНДАРТА *IEEE 802.11b/g/n***

Учебно-методическое пособие
по выполнению лабораторной работы
по дисциплине «Телекоммуникационные системы»
для студентов очной и заочной форм обучения
направлений 11.03.01 «Радиотехника»,
11.03.02 «Инфокоммуникационные технологии и системы связи»
и специальности 11.05.01 «Радиоэлектронные системы
и комплексы»

Севастополь
СевГУ
2019

УДК 621.396 + 621.391
И88

Р е ц е н з е н т:

С.Р. Зиборов - канд. техн. наук, доцент

Ответственный за выпуск:

И.Л. Афонин - д-р техн. наук, профессор,
заведующий кафедрой «Радиоэлектроника и телекоммуникации»

Составитель: Савочкин А.А.

И88 Исследование систем передачи данных стандарта IEEE 802.11b/g/n: учеб.-метод. пособие по выполнению лабораторной работы по дисциплине «Телекоммуникационные системы» для студентов очной и заочной форм обучения направлений 11.03.01 «Радиотехника», 11.03.02 «Инфокоммуникационные технологии и системы связи» и специальности 11.05.01 «Радиоэлектронные системы и комплексы» / Сост. А.А. Савочкин. — Севастополь: СевГУ, 2019. — 29 с.

Целью учебно-методического пособия является оказание помощи студентам в подготовке и выполнении лабораторной работы по дисциплине «Телекоммуникационные системы», а также в получении ими теоретических знаний и практических навыков исследования характеристик оборудования стандарта IEEE 802.11b/g/n.

УДК 621.396+ 621.391

Учебно-методическое пособие утверждено на заседании кафедры «Радиоэлектроника и телекоммуникации», протокол № 10 от 28 марта 2019 г.

Учебно-методическое пособие рассмотрено и рекомендовано к изданию на заседании Ученого совета Института радиоэлектроники и информационной безопасности, протокол № 8 от 30 апреля 2019 г.

СОДЕРЖАНИЕ

1. Цель лабораторной работы.....	4
2. Теоретическая часть.....	4
2.1. Общая характеристика технологий передачи данных для беспроводных сетей.....	4
2.2. Общая характеристика стандартов <i>IEEE 802.11</i>	5
2.3. Физический уровень стандартов <i>IEEE 802.11</i>	7
2.4. Максимальная скорость передачи данных в протоколах <i>IEEE 802.11b/g</i>	11
2.5. Защита данных в беспроводных сетях <i>Wi-Fi</i>	11
3. Описание лабораторной установки	13
3.1. Характеристика аппаратной части	13
3.2. Характеристика программных средств.....	14
4. Порядок выполнения лабораторной работы	16
4.1. Подготовка к выполнению работы	16
4.2. Исследование энергетических характеристик <i>Wi-Fi</i> точек доступа	16
4.3. Исследование пропускной способности сети стандарта <i>IEEE 802.11</i>	17
5. Содержание отчета по лабораторной работе	24
6. Контрольные вопросы	26
6.1. Вопросы для допуска к выполнению лабораторной работы.....	26
6.2. Вопросы для защиты лабораторной работы.....	27
Библиографический список.....	28
Приложение А. Нумерация каналов и частоты стандартов <i>IEEE 802.11a/b/g/n</i>	29

1. ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

Целью лабораторной работы является ознакомление студентов с принципами построения систем беспроводной передачи данных *Wi-Fi* и экспериментальное исследование основных характеристик оборудования стандартов *IEEE 802.11b/g/n*.

2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

2.1. Общая характеристика технологий передачи данных для беспроводных сетей

Технология *Wi-Fi* (*Wireless Fidelity* — «беспроводная точность») определяет принципы организации и функционирования оборудования беспроводных локальных вычислительных сетей (*Wireless Local Area Network, WLAN*).

Установка *WLAN* рекомендуется там, где развёртывание кабельной системы невозможно или экономически нецелесообразно. В настоящее время во многих организациях используется *Wi-Fi*, так как при определённых условиях скорость работы сети уже превышает 100 Мбит/с. Пользователи могут перемещаться между точками доступа по территории покрытия беспроводной сети [1].

Основные преимущества сетей *Wi-Fi*:

- позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания или расширения сети;
- позволяет обеспечить доступ к сети мобильным устройствам;
- *Wi-Fi* устройства разных производителей могут взаимодействовать на базовом уровне сервисов;
- требования *Wi-Fi* реализуются на основе глобальных стандартов, следовательно, *Wi-Fi* оборудование может работать в разных странах по всему миру.

Недостатки сетей *Wi-Fi*:

- частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы. В некоторых странах требуется регистрации сетей *Wi-Fi*, работающих вне помещений;
- высокое по сравнению с другими технологиями потребление энергии, что уменьшает время жизни батарей и повышает температуру устройства;
- стандарт шифрования *WEP* имеет невысокую стойкость алгоритма. Новые устройства поддерживают более совершенные протоколы шифрования данных *WPA* и *WPA2*. Принятие стандарта *IEEE 802.11i* (*WPA2*) в 2004 г. сделало передачу данных более безопасной. Но в некоторых случаях необходимо использовать дополнительное шифрование (например, типа *VPN*) для защиты сети от вторжения;
- *Wi-Fi* имеют ограниченный радиус действия. Типичный домашний маршрутизатор *Wi-Fi* стандарта 802.11b или 802.11g имеет дальность действия около 45 м в помещении и 90 м на открытом пространстве;

— малая пригодность для работы приложений использующих медиа-поток в реальном времени (например, протокол *RTP*, применяемый в *IP*-телефонии).

Примечание. В Российской Федерации, в соответствии с решениями Государственной комиссии по радиочастотам (ГКРЧ) от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия» [2], использование оборудования *Wi-Fi* без получения частного разрешения на использование частот возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий в полосах 2400 — 2483,5 МГц (стандарты 802.11*b* и 802.11*g*) и 5150 — 5350 МГц (802.11*a* и 802.11*n*). Для легального использования внеофисной беспроводной сети *Wi-Fi* (например, радиоканала между двумя соседними домами) необходимо получение разрешения на использование частот (как в полосе 2,4 ГГц, так и 5 ГГц) на основании заключения экспертизы о возможности использования заявленных РЭС.

2.2. Общая характеристика стандартов *IEEE 802.11*

Как и все стандарты группы *IEEE 802*, стандарт 802.11 работает на нижних двух уровнях модели взаимодействия открытых систем (*Open System Interconnection, OSI*): физическом и канальном (рис. 2.1). Любое сетевое приложение, сетевая операционная система, или протокол (например, *TCP / IP*), так же хорошо работают в сети *IEEE 802.11*, как и в сети *Ethernet* [3, 4].

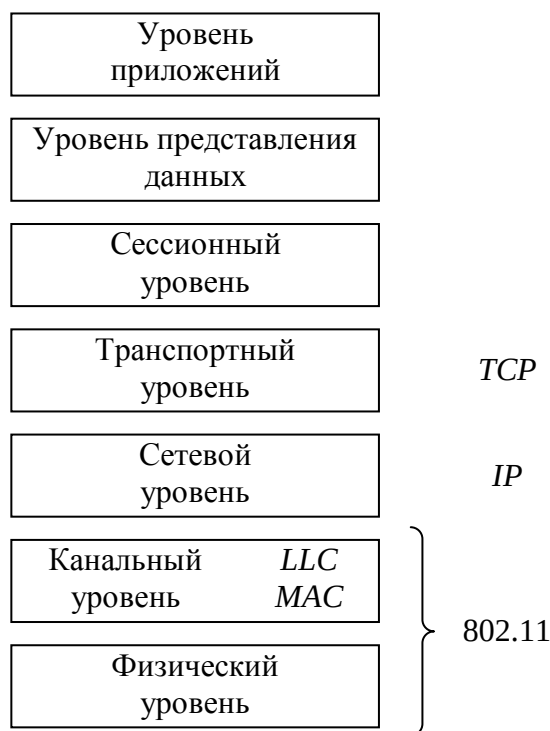


Рис. 2.1 — Уровни модели *OSI* и их соответствие стандарту *IEEE 802.11*

Физический уровень регламентирует передачу информации по физическим каналам и на этом уровне определяются характеристики электрических сигналов.

Канальный уровень определяет создание, передачу и прием кадров данных. Для этого на канальном уровне информационные разряды передаваемых данных группируются в наборы, называемые кадрами. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. В соответствии со спецификацией *IEEE 802.x* канальный уровень делится на два подуровня: управление логическим каналом (*Logical Link Control, LLC*) и управление доступом к среде (*Media Access Control, MAC*). *LLC* обеспечивает обслуживание сетевого уровня, а подуровень *MAC* регулирует доступ к разделяемой физической среде.

Одной из задач канального уровня является проверка доступности среды передачи, а другой — является реализация механизмов обнаружения и коррекции ошибок путем добавления контрольной суммы к кадру [5].

Стандарт *IEEE 802.11* определяет два режима работы сети — режим инфраструктуры — *infrastructure mode* (или клиент-сервер) и режим «*Ad-hoc*» (также называемый точка-точка). В режиме клиент-сервер (как показано на рис. 2.2, а) беспроводная сеть состоит из как минимум одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных оконечных станций. Такая конфигурация носит название базового набора служб (*Basic Service Set, BSS*). Два или более *BSS*, образующих единую подсеть, формируют расширенный набор служб (*Extended Service Set, ESS*). Так как большинству беспроводных станций требуется получать доступ к файловым серверам, принтерам, Интернет, доступным в проводной локальной сети, они будут работать в режиме клиент-сервер.

Режим «*Ad-hoc*» (в переводе с латинского означает — на данный случай, в этой связи, предназначенный только для данной цели) — это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования специальной точки доступа (как показано на рис. 2.2, б). В этом случае для работы сети обеспечивается независимый базовый набор служб (*Independent Basic Service Set, IBSS*).

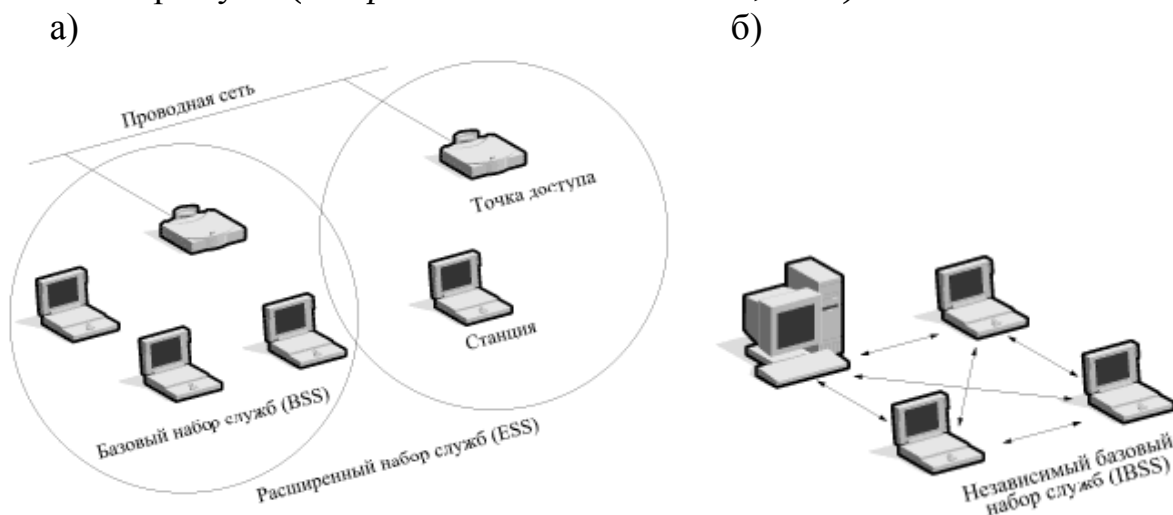


Рис. 2.2 — Архитектура сети а) «клиент-сервер» и б) «точка-точка»

Такой режим полезен в том случае, если инфраструктура беспроводной сети не создана (например, гостиница, выставочный зал, аэропорт), либо по каким-то причинам не может быть сформирована.

2.3. Физический уровень стандартов *IEEE 802.11*

В беспроводных протоколах семейства *IEEE 802.11* используется метод расширения спектра (*Spread Spectrum, SS*). Данная технология подразумевает, что исходный узкополосный информационный сигнал при передаче преобразуется таким образом, что его спектр оказывается значительно шире спектра первоначального сигнала. В результате максимальная спектральная энергетическая плотность преобразованного сигнала оказывается значительно ниже спектральной энергетической плотности исходного сигнала. При этом уровень полезного информационного сигнала может оказаться на уровне естественного шума [6].

Метод расширения спектра заключается в изменении спектральной энергетической плотности сигнала. Необходимо использовать такой способ передачи информации, при котором сигналы различных пользователей могли бы сосуществовать в одном частотном диапазоне и при этом не мешать друг другу. Именно эту задачу и решает метод расширения спектра.

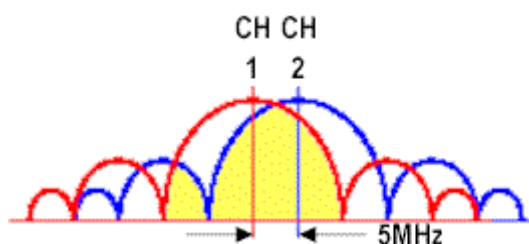
Существует несколько различных методов расширения спектра. В начальном варианте протокола 802.11 используется технология расширения спектра методом прямой последовательности (*Direct Sequence Spread Spectrum, DSSS*) [3].

Стандарт *IEEE 802.11*

В стандарте *IEEE 802.11* предусмотрено два скоростных режима: 1 и 2 Мбит/с. Для кодирования данных на физическом уровне используется метод *DSSS* с 11-ю разрядными кодами Баркера. При информационной скорости 1 Мбит/с скорость следования отдельных разрядов последовательности Баркера равна 11×10^6 символов/с, а ширина спектра такого сигнала равна 22 МГц. Учитывая, что ширина частотного диапазона для стандарта 802.11 равна 83,5 МГц, получаем, что всего в данном частотном диапазоне можно уместить три неперекрывающихся частотных канала.

Весь частотный диапазон, однако, принято делить на 11 частотных перекрывающихся каналов по 22 МГц, отстоящих друг от друга на 5 МГц. К примеру, первый канал занимает частотный диапазон от 2400 до 2423 МГц при центральной частоте 2412 МГц. Второй канал центрирован относительно частоты 2417 МГц (как показано на рис. 2.3, а), а последний, 11 канал, центрирован относительно частоты 2462 МГц. При таком рассмотрении первый, шестой и 11-й каналы не перекрываются друг с другом и имеют зазор в 3 МГц друг относительно друга. Именно эти три канала могут использоваться независимо друг от друга (как показано на рис. 2.3, б).

а)



б)

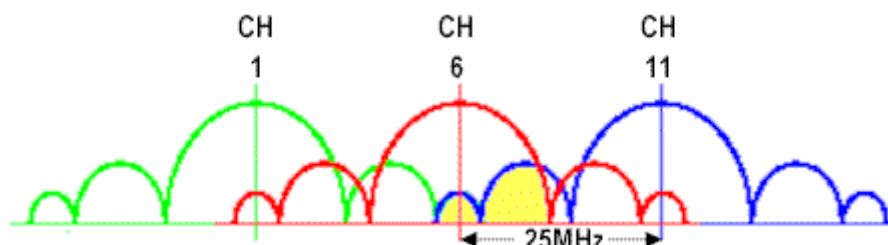


Рис. 2.3 — Перекрывание частотных каналов а) перекрывание соседних каналов, б) частичное перекрывание независимых каналов

Для модуляции несущего сигнала используется относительная двоичная фазовая модуляция (*Differential Binary Phase Shift Key, DBPSK*). При этом кодирование информации происходит за счет сдвига фазы синусоидального сигнала по отношению к предыдущему состоянию сигнала.

Информационная скорость 1 Мбит/с является обязательной в стандарте 802.11, но опционально возможна и скорость в 2 Мбит/с. Для передачи данных на такой скорости используется та же технология *DSSS* (с кодами Баркера), но для модуляции применяется относительная квадратурная фазовая модуляция (*Differential Quadrature Phase Shift Key, DQPS*). При относительной квадратурной фазовой модуляции сдвиг фаз может принимать четыре различных значения: 0 , $\pi/2$, π и $3\pi/2$.

Стандарт IEEE 802.11b

Стандарт *IEEE 802.11b*, принятый в 1999 г., является расширением базового протокола 802.11 и кроме скоростей 1 и 2 Мбит/с предусматривает скорости 5,5 и 11 Мбит/с. Для работы на скоростях 1 и 2 Мбит/с используются метод расширения спектра с использованием кодов Баркера, а для скоростей 5,5 и 11 Мбит/с — комплементарные коды (*Complementary Code Keying, CCK*).

В стандарте 802.11b применяются комплексные комплементарные восьмизначные последовательности, определенные на множестве комплексных элементов.

Использование *CCK* кодов позволяет кодировать восемь разрядов (8 бит) на один символ при скорости 11 Мбит/с и четыре разряда (4 бит) на один символ при скорости 5,5 Мбит/с. При этом в обоих случаях символьная скорость передачи составляет $11/8 = 5,5/4 = 1,385 \times 10^6$ символов в секунду. Соответственно, и ширина спектра сигнала как при скорости 11 Мбит/с и 5,5 Мбит/с составляет 22 МГц.

В стандарте *IEEE 802.11b* также используется двоичное пакетное сверточное кодирование (*Packet Binary Convolutional Coding, PBCC*), при котором входящая последовательность информационных разрядов преобразуется в сверточном кодере таким образом, чтобы каждому входному разряду соответствовало более одного выходного [3]. То есть сверточный кодер добавляет определенную избыточную информацию к исходной последовательности. Если, к примеру, каждым двум входным разрядам соответствует три выходных, то скорость сверточного кодирования будет составлять $2/3$.

В стандарте *IEEE 802.11b* для модуляции предусмотрена либо двоичная (*BDPSK*), либо квадратурная (*QDPSK*) относительная фазовая модуляция.

Информационные и модуляционные характеристики стандарта *IEEE 802.11b* приведены в табл. 2.1 [6].

Таблица 2.1 — Информационные и модуляционные характеристики стандарта *IEEE 802.11b*

Скорость передачи информации, Мбит/с		Метод кодирования	Вид модуляции	Скорость сверточного кодирования	Символьная скорость, 10^6 символ/с	Количество бит в одном символе
1	Обязательная	Код Баркера	<i>DBPSK</i>	—	1	1
2	Обязательная	Код Баркера	<i>DQPSK</i>	—	1	2
5, 5	Обязательная	<i>CCK</i>	<i>DQPSK</i>	—	1,375	4
	Дополнительная	<i>PBCC</i>	<i>DBPSK</i>	$1/2$	11	0,5
11	Обязательная	<i>CCK</i>	<i>DQPSK</i>	—	1,375	8
	Дополнительная	<i>PBCC</i>	<i>DQPSK</i>	$1/2$	11	1

Стандарт *IEEE 802.11g*

Стандарт *IEEE 802.11g* является дальнейшим развитием стандарта *802.11b* и предписывает передачу данных в том же частотном диапазоне, но с более высокими скоростями. Кроме того, стандарт *802.11g* полностью совместим с *802.11b*. Максимальная скорость передачи информации в стандарте *802.11g* составляет 54 Мбит/с.

При разработке стандарта *IEEE 802.11g* рассматривались несколько методов кодирования: ортогонального частотного разделения с мультиплексированием (*Orthogonal Frequency Division Multiplexing, OFDM*), и двоичного пакетного сверточного кодирования *PBCC*, опционально реализованный в стандарте *802.11b*. В результате в стандарте *802.11g* для кодирования применяются методы *OFDM* и *CCK*, а опционально предусмотрено использование *PBCC*.

Метод *OFDM* заключается в том, что поток передаваемых данных распределяется по множеству частотных подканалов и передача ведется параллельно на всех этих подканалах. При этом высокая скорость передачи достигается именно за счет одновременной передачи данных по всем каналам, хотя

скорость передачи в отдельном подканале невысока, что и создает предпосылки для подавления межсимвольной интерференции.

В стандарте *IEEE 802.11g* на низких скоростях передачи используется фазовая модуляция с абсолютным кодированием, то есть двоичная и квадратурная фазовые модуляции *BPSK* и *QPSK*. При использовании *BPSK* модуляции в одном символе кодируется только один информационный разряд, а при использовании *QPSK* модуляции — два информационных разряда.

При модуляции *BPSK* скорость передачи данных равна 6 и 9 Мбит/с, а при модуляции *QPSK* — 12 и 18 Мбит/с.

Для передачи на более высоких скоростях применяют квадратурную амплитудную модуляцию (*Quadrature Amplitude Modulation, QAM*), при которой сообщение кодируется за счет изменения фазы и амплитуды сигнала. В протоколе *802.11g* используется модуляция 16-QAM и 64-QAM. В случае использования 16 состояний сигнала обеспечивается кодирование четыре двоичных разряда в одном сигнале. При 64 возможных состояниях сигнала кодируется шесть двоичных разрядов в одном сигнале. Модуляция 16-QAM применяется на скоростях 24 и 36 Мбит/с, а модуляция 64-QAM — на скоростях 48 и 54 Мбит/с.

Соответствие скоростей передачи, методов кодирования и модуляции для стандарта *802.11g* приведены в табл. 2.2 [6].

Таблица 2.2 — Соответствие скоростей передачи и методов кодирования для стандарта *IEEE 802.11g*

Скорость передачи, Мбит/с		Метод кодирования	Вид модуляции
1	Обязательная	Код Баркера	<i>DBPSK</i>
2	Обязательная	Код Баркера	<i>DQPSK</i>
5,5	Обязательная	<i>CCK</i>	<i>DQPSK</i>
	Дополнительная	<i>PBCC</i>	<i>DBPSK</i>
6	Обязательная	<i>OFDM</i>	<i>BPSK</i>
	Дополнительная	<i>CCK-OFDM</i>	<i>BPSK</i>
9	Дополнительная	<i>OFDM, CCK-OFDM</i>	<i>BPSK</i>
11	Обязательная	<i>CCK</i>	<i>DQPSK</i>
	Дополнительная	<i>PBCC</i>	<i>DQPSK</i>
12	Обязательная	<i>OFDM</i>	<i>QPSK</i>
	Дополнительная	<i>CCK-OFDM</i>	<i>QPSK</i>
18	Дополнительная	<i>OFDM, CCK-OFDM</i>	<i>QPSK</i>
22	Дополнительная	<i>PBCC</i>	<i>DQPSK</i>
24	Обязательная	<i>OFDM</i>	16-QAM
	Дополнительная	<i>CCK-OFDM</i>	нет данных
33	Дополнительная	<i>PBCC</i>	нет данных
36	Дополнительная	<i>OFDM, CCK-OFDM</i>	16-QAM
48	Дополнительная	<i>OFDM, CCK-OFDM</i>	64-QAM
54	Дополнительная	<i>OFDM, CCK-OFDM</i>	64-QAM

2.4. Скорость передачи данных в стандарте *IEEE 802.11b/g*

Максимальная скорость, определяемая стандартом *IEEE 802.11b*, составляет 11 Мбит/с, а для *IEEE 802.11g* — 54 Мбит/с. Однако следует четко различать полную скорость передачи и эффективную скорость передачи. Дело в том, что технология доступа к среде передачи данных, структура передаваемых кадров, заголовки, прибавляемые к передаваемым кадрам на различных уровнях модели *OSI*, — все это предполагает наличие достаточно большого объема служебной информации. В результате эффективная скорость передачи, то есть скорость выдачи данных получателю, всегда оказывается ниже полной скорости передачи.

Более того, реальная скорость передачи зависит и от структуры беспроводной сети. Так, если все клиенты сети используют один и тот же протокол, например *802.11g*, то сеть является гомогенной и скорость передачи данных в такой сети выше, чем в смешанной сети, где имеются клиенты как *802.11g*, так и *802.11b*.

Кроме того, реальная скорость передачи данных зависит и от используемого протокола (*TCP* или *UDP*) и от размера длины пакета. Протокол *UDP* обеспечивает более высокие скорости передачи. Теоретические максимальные скорости передачи данных для различных типов сетей и протоколов представлены в табл. 2.3 [7].

Таблица 2.3 — Максимальные скорости передачи информации для различных типов сетей и протоколов при величине пакетов 1500 байт

Тип сети	Модуляция	Максимальная скорость, Мбит/с	Теоретическая максимальная скорость передачи по протоколу <i>TCP</i> , Мбит/с	Теоретическая максимальная скорость передачи по протоколу <i>UDP</i> , Мбит/с
802.11b	<i>CCK</i>	11	5,9	7,1
802.11g совместно с 802.11b	<i>OFDM/CCK</i>	54	14,4	19,5
802.11g	<i>OFDM/CCK</i>	54	24,4	30,5

2.5. Защита данных в беспроводных сетях *Wi-Fi*

Стандарт *IEEE 802.11b* обеспечивает контроль доступа на *MAC*-уровне (второй уровень в модели *OSI*), и механизмы шифрования, известные как *Wired Equivalent Privacy (WEP)*, целью которых является обеспечение беспроводной сети средствами безопасности, эквивалентными средствам безопасности проводных сетей. Когда включен *WEP*, он защищает только пакет данных, но не защищает заголовки физического уровня, так что другие станции в сети могут просматривать данные, необходимые для управления сетью.

WEP использует алгоритм шифрования *Rivest Cipher 4 (RC4)* с 40 или 104-битным ключом. При включении *WEP* все станции (как клиентские, так и точки доступа) получают свой ключ, который применяется для шифрования данных, прежде чем последние будут переданы на передатчик. Если станция получает пакет, не зашифрованный соответствующим ключом, то он игнорируется.

В настоящее время считается, что криптостойкость *WEP* кодирования недостаточна, поскольку при *WEP* кодировании используются слишком похожие ключи для различных пакетов данных.

WPA и *WPA2 (Wi-Fi Protected Access)* — представляет собой метод сертификации устройств беспроводной связи. Технология *WPA* пришла на замену технологии *WEP*. Преимуществами *WPA* являются усиленная безопасность данных и более жесткий контроль доступа к беспроводным сетям.

В стандарте *WPA* используется расширяемый протокол аутентификации (*Extensible Authentication Protocol, EAP*) как основа для механизма аутентификации пользователей. Для проверки прав пользователь проходит проверку по специальной базе зарегистрированных пользователей. Без аутентификации работа в сети для пользователя будет запрещена.

База зарегистрированных пользователей и система проверки в больших сетях чаще всего расположены на специальном сервере (например, типа *RADIUS*).

Но следует отметить, что *WPA* имеет и упрощённый режим. Этот режим получил название *Pre-Shared Key (WPA-PSK)*. При применении режима *WPA-PSK* необходимо ввести один пароль для каждого отдельного узла беспроводной сети (беспроводные маршрутизаторы, точки доступа, мосты и т. д.). Если пароль совпадает с записями в устройстве беспроводного доступа, пользователь получит разрешение на доступ в сеть. При этом механизмы шифрования, которые используются для *WPA* и *WPA-PSK*, являются идентичными. Единственное отличие *WPA-PSK* состоит в том, что аутентификация производится с использованием пароля, а не по сертификату пользователя. Процедура *WPA2* регламентируется стандартом 802.11i, который был принят в 2004 г. Данный метод призван заменить *WPA*. В нём реализовано шифрование (*Advanced Encryption Standard, AES*), за счет чего *WPA2* стал более защищенным, чем свой предшественник. С 2006 г. поддержка *WPA2* стала обязательным условием для всех сертифицированных *Wi-Fi* устройств. Кроме того, для контроля доступа в каждой точке доступа назначается идентификатор сети (*SSID*), без знания которого мобильная станция не сможет подключиться к базовой станции. Дополнительно базовая станция может хранить список разрешённых *MAC* адресов, называемый списком контроля доступа, разрешая доступ только тем клиентам, чьи *MAC* адреса находятся в списке.

3. ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

3.1. Характеристика аппаратной части

Конфигурация сети и состав оборудования для выполнения лабораторной работы изображен на рис. 3.1. Исследование производится с использованием двух стационарных компьютеров и трех точек доступа (модем *ORiNOCO*, роутеры *D-link DIR-400* и *D-link DIR-300NRU*), с которыми поочередно устанавливается соединение в режиме клиент-сервер. Все исследования производятся с использованием портативного компьютера.

Вариант соединения А — точка доступа с использованием модема *ORiNOCO*, подключенный к стационарному компьютеру с помощью *USB* интерфейса. На компьютере организован сервер раздачи *IP* адресов (*DHCP*) в диапазоне 192.168.1.50 — 192.168.1.59. Собственный *IP* адрес *USB* модема *ORiNOCO* — 192.168.1.2. Конечная точка тестирования — стационарный компьютер с *IP* адресом *USB* адаптера 192.168.1.2. Стационарный компьютер расположен в аудитории Б401.

Вариант соединения Б — точка доступа на основе аппаратного роутера *D-link DIR-300NRU* на котором включен режим раздачи *IP* адресов в диапазоне 192.168.20.50 — 192.168.20.59.

К сети кафедры роутер подключен по интерфейсу *Wide Area Network* (*WAN*), т. е. передача данных при выполнении лабораторной работы производится через сетевой экран устройства (фаервол). Собственный *IP* адрес роутера в локальной сети *LAN* — 192.168.20.1.

Конечная точка тестирования — стационарный компьютер с *IP* адресом 192.168.20.2 (расположен в аудитории Б401).

Вариант соединения В — точка доступа на основе аппаратного роутера *D-link DIR-300NRU* на котором включен режим раздачи *IP* адресов в диапазоне 192.168.20.50 — 192.168.20.59. Собственный *IP* адрес роутера в локальной сети — 192.168.20.1.

К сети кафедры роутер подключен по интерфейсу *WAN*, т.е. передача данных при выполнении лабораторной работы производится через сетевой экран устройства (фаервол). Собственный *IP* адрес роутера в локальной сети *WAN* — 192.168.20.1. Конечная точка тестирования — стационарный компьютер с *IP* адресом 192.168.0.1 (расположен в аудитории Б405).

Вариант соединения Г — точка доступа на основе аппаратного роутера *D-link DIR-400*. *IP* адрес в этом случае формируется *DHCP* сервером кафедры в диапазоне 192.168.0.240 — 192.168.0.249.

К сети кафедры роутер подключен по интерфейсу *Local area network* (*LAN*), т.е. передача данных при выполнении лабораторной работы через сетевой экран устройства (фаервол) не производится. Собственный *IP* адрес роутера в локальной сети *LAN* — 192.168.0.11. Конечная точка тестирования — стационарный компьютер с *IP* адресом 192.168.20.2 (расположен в аудитории Б401).

Вариант соединения Д — точка доступа на основе аппаратного роутера *D-link DIR-400*. *IP* адрес в этом случае формируется *DHCP* сервером кафедры в диапазоне 192.168.0.240 — 192.168.0.249.

К сети кафедры роутер подключен по интерфейсу *LAN*, т.е. передача данных при выполнении лабораторной работы через сетевой экран устройства (фаервол) не производится. Собственный *IP* адрес роутера в локальной сети *LAN* — 192.168.0.11. Конечная точка тестирования — стационарный компьютер с *IP* адресом 192.168.0.1 (расположен в аудитории Б405).

3.2. Характеристика программных средств

Для выполнения работы используется программное обеспечение (ПО) *Chariot*, которое разработано для тестирования сетей типа клиент-сервер, и генерирует потоки данных по типу «запрос-ответ... запрос-ответ». По сути *Chariot* — это комплекс эталонных тестов, которые представляют собой фиксированные процедуры. Комплект тестов этого пакета выполняет простые операции чтения и записи файлов для имитации работы файлового сервера (например, команды *ftp* протокола — *put*, *get*), а также имитирует передачу данных в *World Wide Web*. ПО *Chariot* состоит из консоли *Chariot* и оконечных программных агентов *Endpoint*.

Консоль реализует интерфейс с тестовой системой. Именно с помощью командной консоли осуществляется компоновка и администрирование выполняемых тестов. Оконечные программные агенты *Endpoint* устанавливаются на тех сетевых узлах, которые включаются в процесс тестирования сети. Например, если интересно, насколько хорошо файловый сервер способен поддерживать группу сетевых клиентов, то агентов следует установить на сервере и на каждом клиенте. Причем консоль управления устанавливается лишь на один компьютер (с которого производится тестирование), а *Endpoint* на все компьютеры, между которыми предполагается проводить измерения. Важно, что ПО *Chariot* понимает несколько сетевых протоколов, в том числе *UDP*, *TCP*, *IPX*, *SPX* и *APPC* (*Advanced Program-to-Program Communications*) компании *IBM*. Один конечный пункт выполняет роль клиента, а другой — сервера. При настройке тестов *Chariot* выбираются конечные пункты «*Endpoint 1*» и «*Endpoint 2*». Для имитации работы реальной сети допускается задание в любом тесте нескольких пар одновременно взаимодействующих конечных пунктов. В зависимости от характера теста, каждая пара конечных пунктов может выполнять свой сценарий тестирования или работать по единому сценарию.

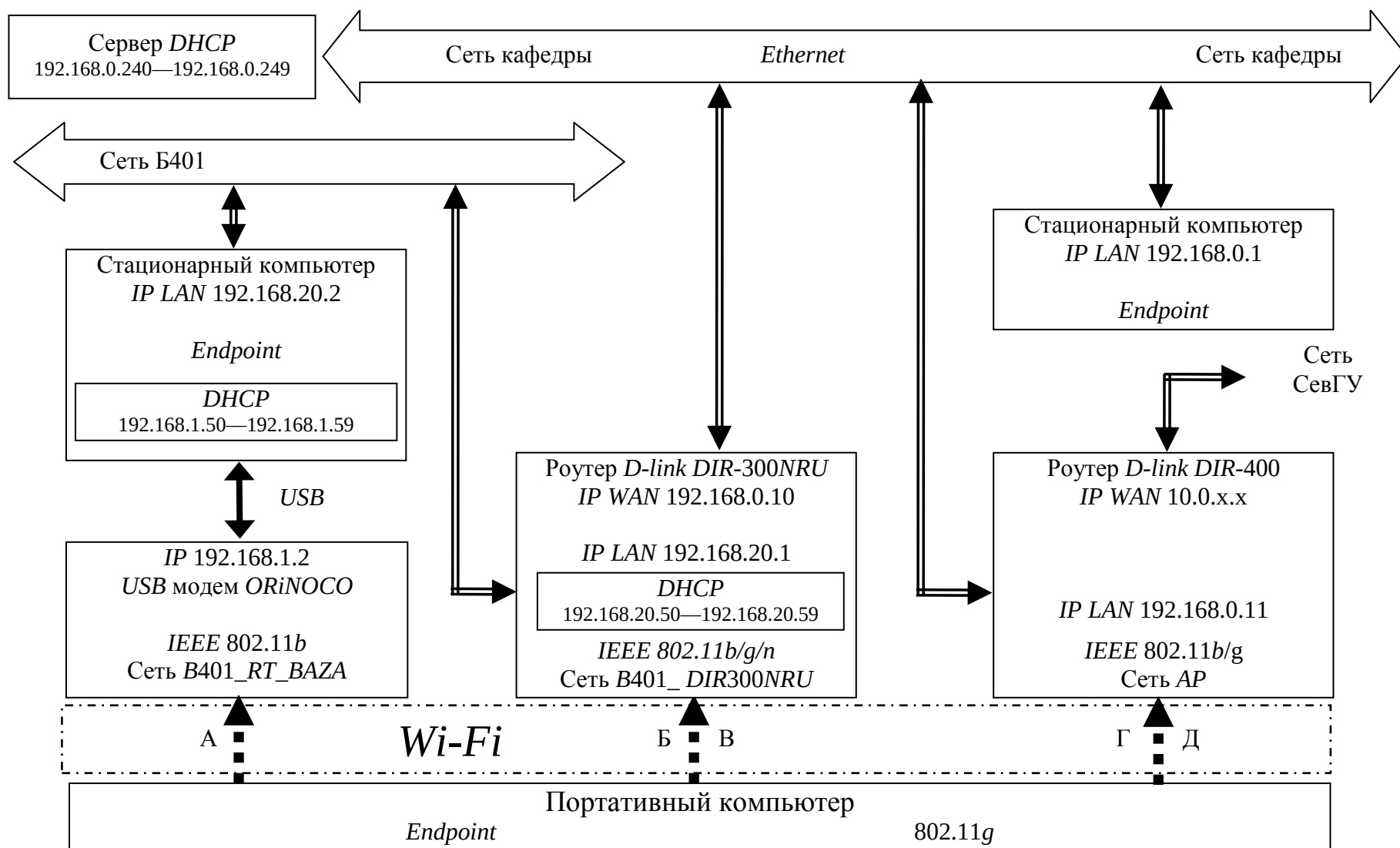


Рис. 3.1 — Структурная схема лабораторного оборудования

4. ПОРЯДОК ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

4.1. Подготовка к выполнению работы

1) Включить стационарный компьютер-сервер с точкой доступа *ORiNOCO*. Для корректного запуска программного обеспечения сервера, необходимо, чтобы точка доступа была подключена к системному блоку кабелем *USB* до включения компьютера.

2) Проверить включение аппаратного роутера *D-link* типа *DIR-300NRU*.

3) Портативный компьютер после запуска операционной системы готов к проведению исследований.

4.2. Исследование энергетических характеристик *Wi-Fi* точек доступа

1) Произвести запуск программы *inSSIDer*, которая сканирует диапазон частот 2,4 ГГц и показывает работающие в данном месте беспроводные точки доступа и адаптеры, работающие в режиме *Ad-Hoc*. Программа *inSSIDer* выдает информацию о *MAC*-адресах обнаруженных беспроводных устройств, значения идентификатора сети *SSID*, имена устройств, используемые частотные каналы, сообщает о том, включен ли режим шифрования и т. д. Вид основного окна программы *inSSIDer* показан на рис. 4.1.

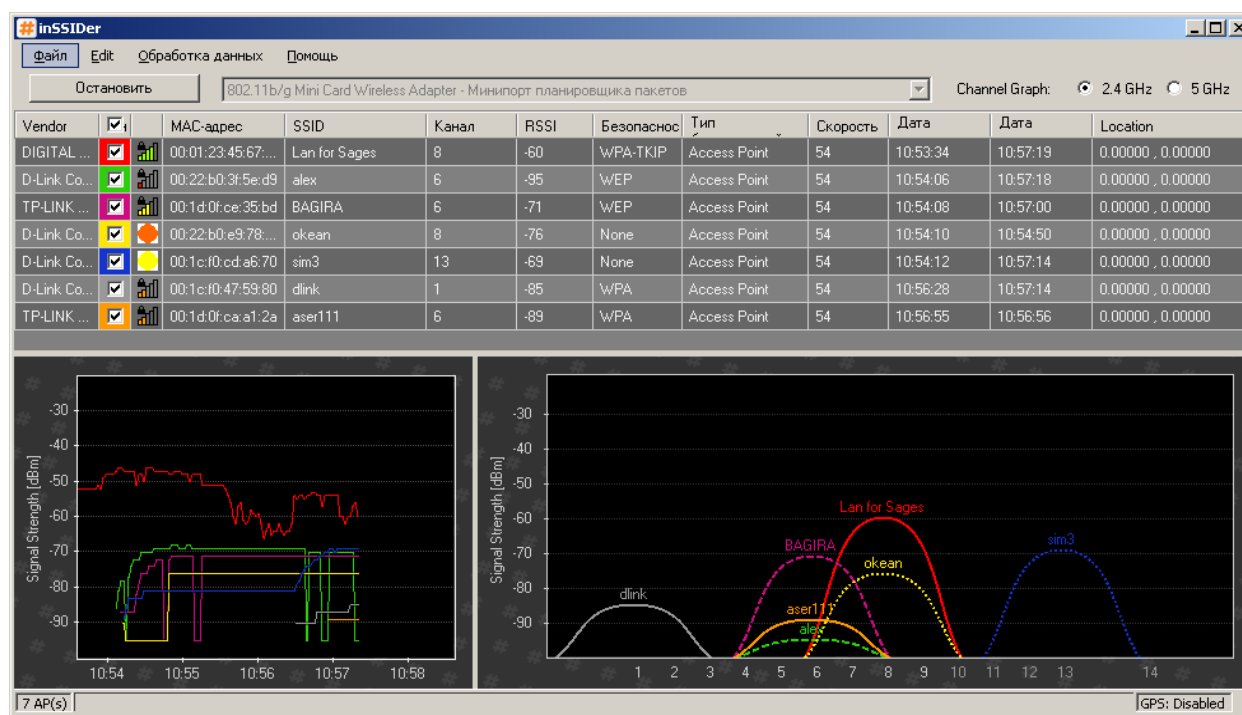


Рис. 4.1 — Вид основного окна программы *inSSIDer*

2) Определить уровень мощности сигнала и отношение сигнал-шум для всех доступных беспроводных средств. Сканирование проводить в течение 2...3 минут. Для каждой точки доступа измерить значения уровня мощности. Зафиксировать полную информацию, включая номера частотных каналов для всех доступных точек доступа. Завершить работу программы *inSSIDer*.

4.3. Исследование пропускной способности сети стандарта 802.11

Эта часть работы выполняется по вариантам в соответствии с табл. 4.1.

Таблица 4.1 — К выбору варианта для проведения исследования

Последняя цифра номера зачетной книжки	0	1	2	3	4	5	6	7	8	9
Задание 1	А	А	Б	Б	В	В	А	А	Г	Б
Задание 2	Б	В	В	Г	Г	Д	Г	Д	Д	Д

Вариант соединения А

1) **Произвести соединение с сетью B401_RT_BAZA.** Конфигурация сети показана на рис. 3.1. Для организации этой сети используется точка доступа расположенная в аудитории Б401 (стационарный компьютер-сервер с точкой доступа *ORiNOCO*).

Для этого нажать правой кнопкой мыши на значке беспроводного сетевого соединения в правой части панели задач, и выбрать команду «Просмотр доступных беспроводных сетей». Далее в окне беспроводного сетевого соединения операционной системы *Windows XP* выбрать левой кнопкой мыши соединение *B401_RT_BAZA* и нажать кнопку «Подключить». Вид окна показан на рис. 4.2.

При появлении запроса на ввод ключа сети дважды ввести последовательность символов 1234567890, и подтвердить ввод ключа, нажав кнопку «Подключить». Вид окна ввода ключевой последовательности показан на рис. 4.3.

Внимание! В случае ошибки при вводе ключевой последовательности доступ к точке доступа не будет получен.

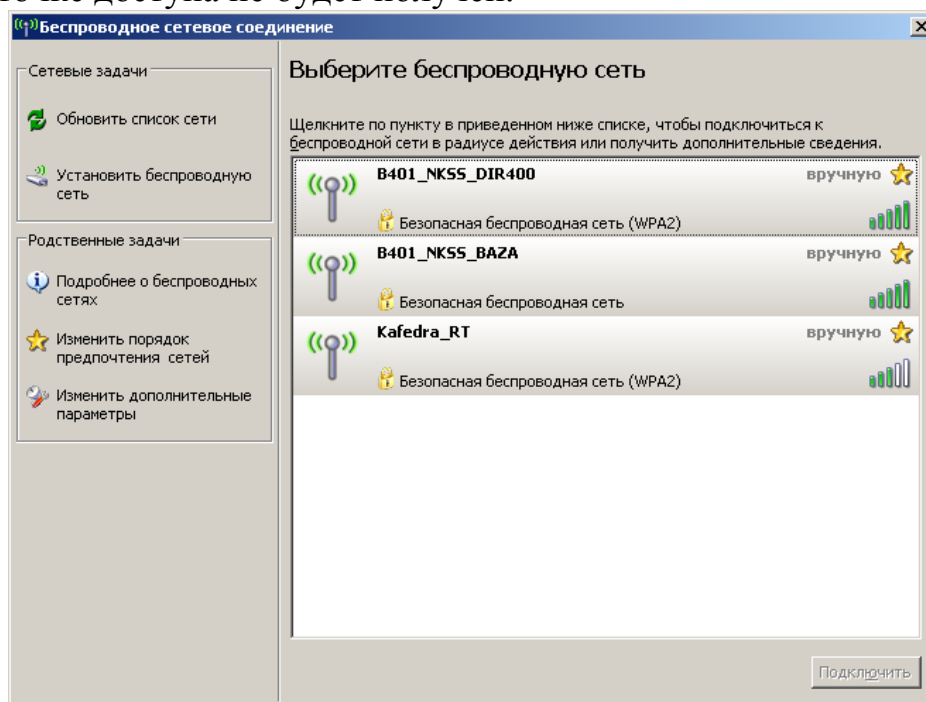


Рис. 4.2 — Вид окна беспроводного сетевого соединения операционной системы *Windows*

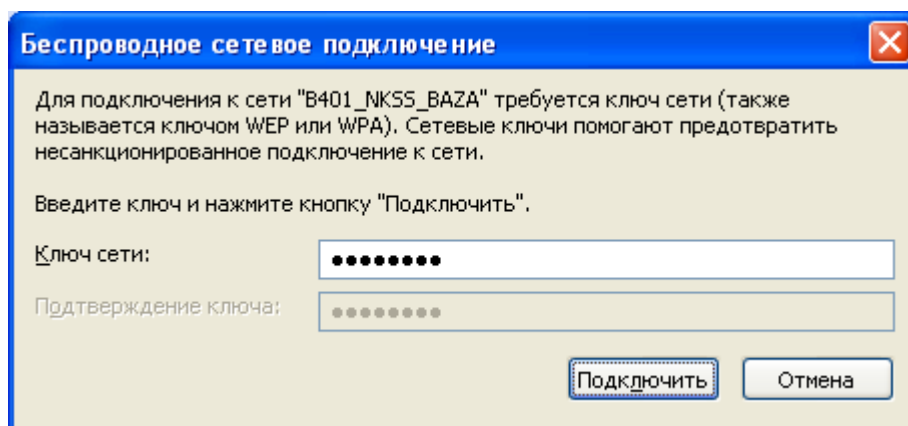


Рис. 4.3 — Вид окна ввода ключевой последовательности WEP или WPA

2) **Произвести запуск командной консоли Windows.** Для этого нажать «Пуск» — «Выполнить», и в поле ввода команды набрать *CMD*, завершив ввод нажатием кнопки *OK*.

Определить назначенный сервером *IP* адрес, для этого ввести и выполнить команду *IPCONFIG*. Адрес компьютера должен быть в диапазоне сети 192.168.*.*.

Если *IP* адрес не попадает в указанный диапазон, то следует проверить физическое подключение *USB* адаптера *ORiNOCO* к стационарному компьютеру и перезагрузить стационарный компьютер-сервер.

Проверить на портативном компьютере наличие соединения с компьютером-сервером с помощью команды *ping* 192.168.1.2. Зафиксировать в отчет среднее значение временной задержки отклика.

3) **Измерить пропускную способность сети.** Для этого использовать специализированное ПО *Chariot*, которое состоит из консоли управления измерениями и «конечных точек производительности» — «*Endpoint*».

Произвести запуск программы тестирования сетей *Chariot*, и создать новый тест (команда *New*). Вид главного окна программы *Chariot* показан на рис. 4.4.

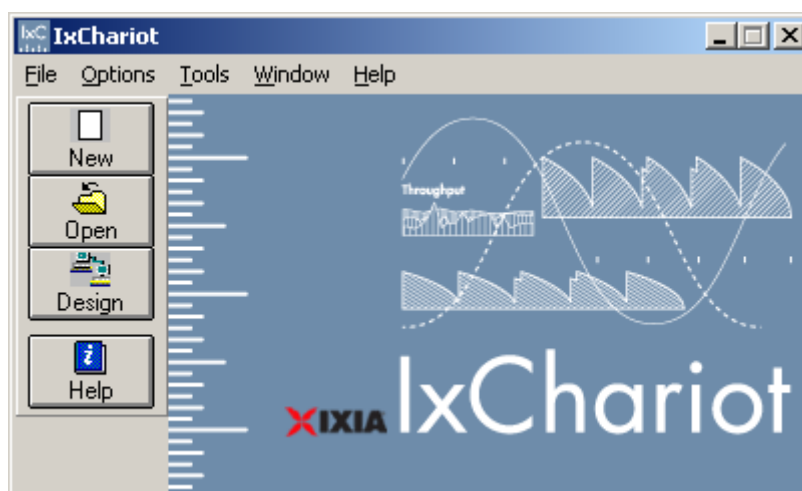


Рис. 4.4 — Вид главного окна программы *Chariot*

В окне «*IxChariot Test*» необходимо выбрать конфигурацию для сетевого тестирования — указать пару узлов, между которыми будет передаваться трафик. Для этого необходимо нажать «*Add pair*» (рис. 4.5).

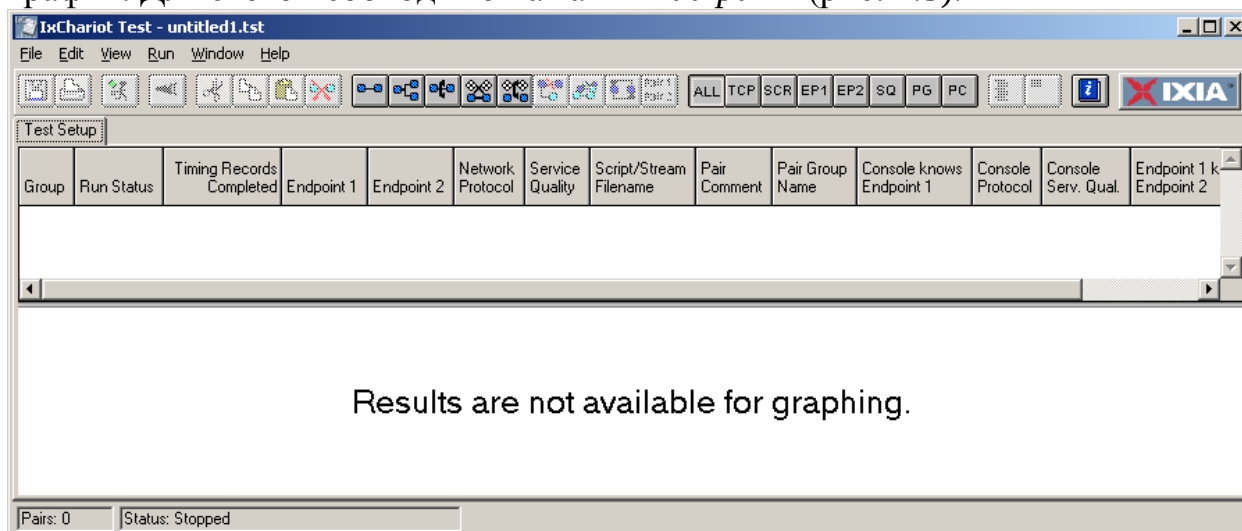


Рис. 4.5 — Вид окна конфигурирования нового теста

В следующем окне (рис. 4.6) следует задать *IP* адреса точек сети: «*Endpoint 1 network address*» — 192.168.1.2 и «*Endpoint 2 network address*» — *IP* адрес портативного компьютера, а в поле «*Pair comment*» указать Ф.И.О. студента (как показано на рис. 4.6).

В этом же окне выберите тип сетевого протокола (*Network protocol*) — *TCP* и выберите сценарии проведения измерений «*Throughput.scr*». Поле *Service quality* оставить не заполненным.

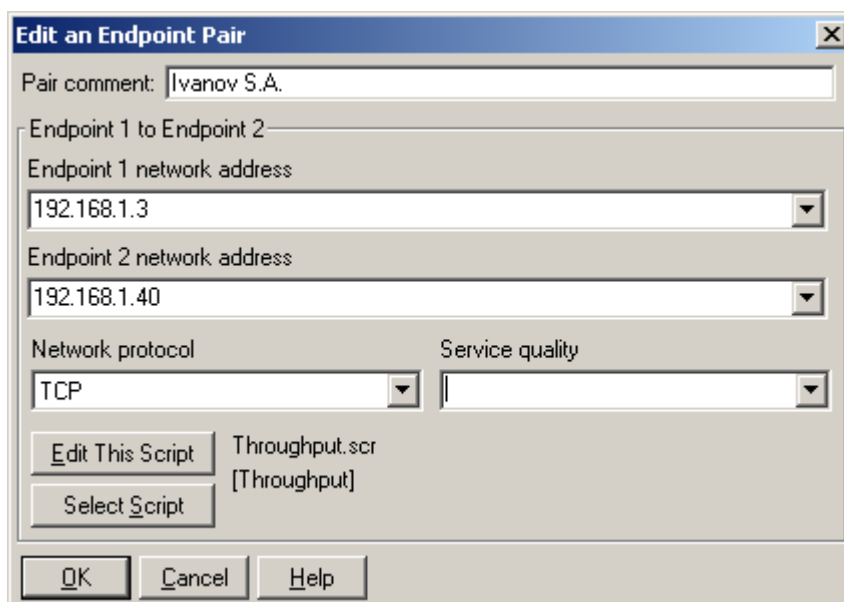


Рис. 4.6 — Вид окна задания параметров тестирования для двух узлов сети

После задания всех параметров теста, следует нажать *OK*. Для выполнения тестирования следует развернуть программу *Chariot* в полноэкранный режим и запустите тест нажатием на кнопку «*Run*» (рис. 4.7).

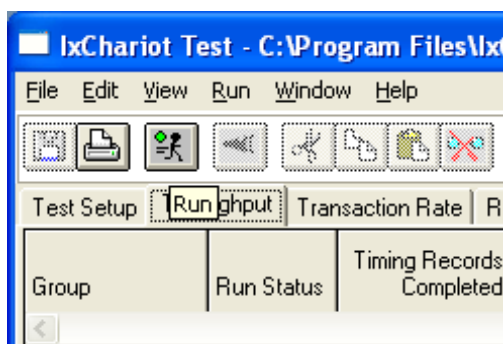


Рис. 4.7 — Запуск теста на выполнение

Результат выполнения теста отобразится в окне, как показано на рис. 4.8. Активировать закладку *Throughput* (пропускная способность) окна «*IxChariot Test*» и сохранить копию экрана тестирования в файл. Для этого рекомендуется при активном окне «*IxChariot Test*» нажать комбинацию клавиш [Alt] - [PrintScreen], и после этого вставить изображение в документ *Microsoft Office Word* или в окно редактора *Paint*.

4) После проведения тестирования активировать закладку *Response Time* окна «*IxChariot Test*» и сохранить копию экрана тестирования в файл.

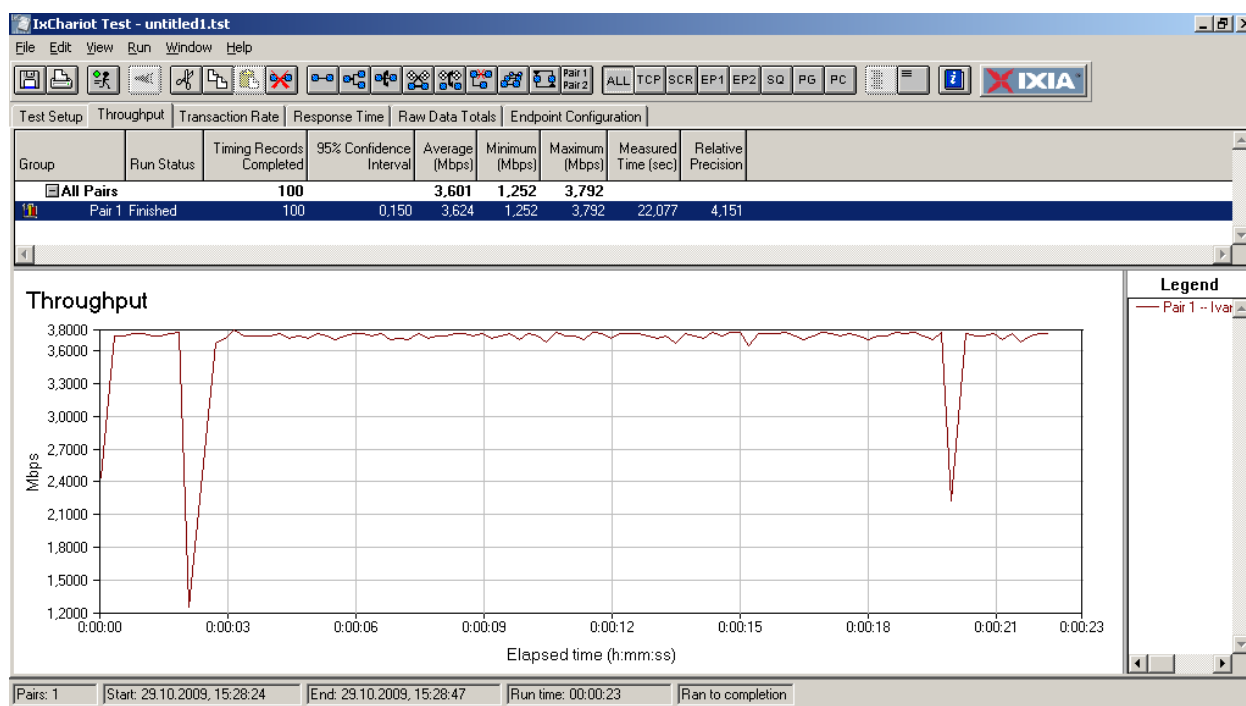


Рис. 4.8 — Результат выполнения теста для двух узлов сети

5) Выполнить отключение от точки доступа. Для этого в окне беспроводного сетевого соединения операционной системы *Windows* выделить соединение *B401_RT_BAZA*, и нажать на кнопку «Разъединить», как показано на рис. 4.9.

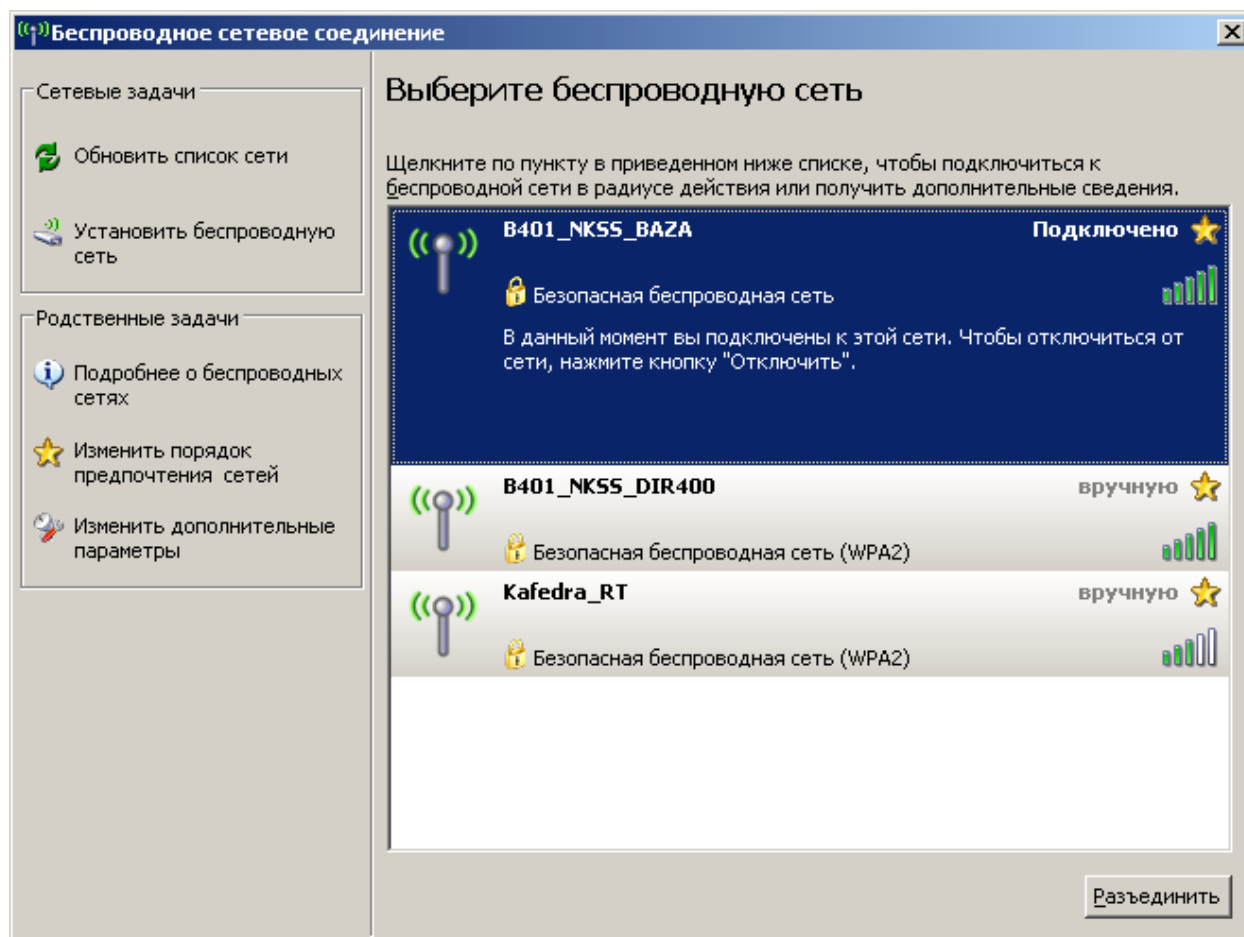


Рис. 4.9 — Вид окна беспроводного сетевого соединения операционной системы *Windows* при отключении от точки доступа

Варианты соединений Б и В

1) **Произвести соединение с сетью *B401_DIR300NRU***. Конфигурация сети показана на рис. 3.1. Для организации этой сети используется аппаратный роутер *DIR300NRU* (расположенный в аудитории Б401) и стационарный компьютер (вариант Б — компьютер в аудитории Б401 с *IP* адресом 192.168.20.2; вариант В — компьютер в аудитории Б405 с *IP* адресом 192.168.0.1).

Для этого нажать правой кнопкой мыши на значке беспроводного сетевого соединения в правой части панели задач, и выбрать команду «Беспроводные сети». Далее в окне беспроводного сетевого соединения операционной системы *Windows* выбрать левой кнопкой мыши соединение *B401_DIR300NRU* и нажать кнопку «Подключить». Вид окна показан на рис. 4.2.

При появлении запроса на ввод ключа сети, не изменяя запомненных значений ключевой последовательности подтвердить ввод ключа, нажав кнопку «Подключить». Вид окна ввода ключевой последовательности показан на рис. 4.3.

Внимание! В случае ввода неверной ключевой последовательности доступ к точке доступа не будет получен.

2) **Произвести запуск командной консоли *Windows*.** Для этого нажать «Пуск» - «Выполнить», и в поле ввода команды набрать *CMD*, завершив ввод нажатием кнопки *ОК*.

Определить назначенный сервером *IP* адрес, для этого выполнить команду *IPCONFIG*. Адрес компьютера должен быть в диапазоне сети 192.168.*.*.

Проверить на портативном компьютере наличие соединения с аппаратным роутером, используя команду *ping* 192.168.20.1.

Повторить команду *ping* для адреса (вариант Б — 192.168.20.2; вариант В — 192.168.0.1). Зафиксировать в отчет минимальное, максимальное и средние значения временных задержек отклика.

3) **Измерить пропускную способность сети.** Для этого использовать специализированное ПО *Chariot*, которое состоит из консоли управления измерениями и «конечных точек производительности» — «*Endpoint*».

Произвести запуск программы тестирования сетей *Chariot*, и создать новый тест (команда *New*). Вид главного окна программы *Chariot* показан на рис. 4.4.

В окне «*IxChariot Test*» необходимо выбрать конфигурацию для сетевого тестирования — указать пару узлов, между которыми будет передаваться трафик. Для этого необходимо нажать «*Add pair*» (рис. 4.5).

В следующем окне (рис. 4.6) следует задать *IP* адреса точек сети: «*Endpoint 1 network address*» — *IP* адрес портативного компьютера и «*Endpoint 2 network address*» — (вариант Б — 192.168.20.2; вариант В — 192.168.0.1).

В этом же окне выберите тип сетевого протокола (*Network protocol*) — *TCP* и выберите сценарии проведения измерений «*Throughput.scr*». Поле *Service quality* оставить не заполненным.

После задания всех параметров теста, нажать *ОК*. Для выполнения тестирования развернуть программу *Chariot* в полноэкранный режим и запустите тест нажатием на кнопку «*Run*» (рис. 4.7).

Результат выполнения теста отобразится в окне, как показано на рис. 4.8. Активировать закладку *Throughput* (пропускная способность) окна «*IxChariot Test*» и сохранить копию экрана тестирования в файл. Для этого рекомендуется при активном окне «*IxChariot Test*» нажать комбинацию клавиш [Alt] - [PrintScreen], и после этого вставить изображение в документ *Microsoft Office Word* или в окно редактора *Paint*.

4) После проведения тестирования активировать закладку *Response Time* окна «*IxChariot Test*» и сохранить копию экрана тестирования в файл.

5) Произвести замену *IP* адресов для используемых точек сети. Для этого сделать двойной щелчок на строчке *Pair 1* окна программы *Chariot*, и установить *IP* адреса точек сети: «*Endpoint 1 network address*» — (вариант Б — 192.168.20.2; вариант В — 192.168.0.1), «*Endpoint 2 network address*» — *IP* адрес портативного компьютера.

Далее по аналогии с п.3 выполнить тестирование сети. Зафиксировать полученный результат в протоколе измерений и далее дать ему объяснение в отчете по лабораторной работе.

6) Выполнить отключение от точки доступа, для этого в окне беспроводного сетевого соединения операционной системы *Windows XP* активировать соединение *B401_DIR300NRU*, и нажать на кнопку «Разъединить», как показано на рис. 4.9.

Варианты соединений Г и Д

1) **Произвести соединение с сетью AP.** Конфигурация сети показана на рис. 3.1. Для организации этой сети используется аппаратный роутер *DIR400* (расположенный в аудитории Б405) и стационарный компьютер (вариант Г — компьютер в аудитории Б401 с *IP* адресом 192.168.20.2; вариант Д — компьютер в аудитории Б405 с *IP* адресом 192.168.0.1).

Для этого нажать правой кнопкой мыши на значке беспроводного сетевого соединения в правой части панели задач, и выбрать команду «Беспроводные сети». Далее в окне беспроводного сетевого соединения операционной системы *Windows XP* выбрать левой кнопкой мыши соединение с именем *AP* и нажать кнопку «Подключить». Вид окна показан на рис. 4.2.

При появлении запроса на ввод ключа сети, не изменяя запомненного значения ключевой последовательности подтвердить ввод ключа, нажав кнопку «Подключить». Вид окна ввода ключевой последовательности показан на рис. 4.3.

Внимание! В случае ввода неверной ключевой последовательности доступ к точке доступа не будет получен.

2) **Произвести запуск командной консоли *Windows*.** Для этого нажать кнопку «Пуск» и команду «Выполнить», и в поле ввода команды набрать *CMD*, завершив ввод нажатием кнопки *OK*.

Определить назначенный сервером *IP* адрес, для этого выполнить команду *IPCONFIG*. Адрес компьютера должен быть в диапазоне сети 192.168.*.*.

Проверить на портативном компьютере наличие соединения с аппаратным роутером используя команду *ping* 192.168.0.11.

Повторить команду *ping* для адреса (вариант Г — 192.168.20.2; вариант Д — 192.168.0.1). Зафиксировать в отчет минимальное, максимальное и средние значения временных задержек отклика.

3) **Измерить пропускную способность сети.** Для этого использовать специализированное ПО *Chariot*, которое состоит из консоли управления измерениями и «конечных точек производительности» — «*Endpoint*».

Произвести запуск программы тестирования сетей *Chariot*, и создать новый тест (команда *New*). Вид главного окна программы *Chariot* показан на рис. 4.4.

В окне «*IxChariot Test*» необходимо выбрать конфигурацию для сетевого тестирования — указать пару узлов, между которыми будет передаваться трафик. Для этого необходимо нажать «*Add pair*» (рис.4.5).

В следующем окне (рис. 4.6) следует задать *IP* адреса точек сети: «*Endpoint 1 network address*» — (вариант Г — 192.168.20.2; вариант Д — 192.168.0.1) и «*Endpoint 2 network address*» — *IP* адрес портативного компьютера (как показано на рис. 4.6).

В этом же окне выберите тип сетевого протокола (*Network protocol*) — *TCP* и выберите сценарии проведения измерений «*Throughput.scr*». Поле *Service quality* оставить не заполненным.

После определения всех параметров теста, нажать *OK*. Для выполнения тестирования развернуть программу *Chariot* в полноэкранный режим и запустите тест нажатием на кнопку «*Run*» (рис. 4.7).

Результат выполнения теста отобразится в окне, как показано на рис. 4.8. Активировать закладку *Throughput* (пропускная способность) окна «*IxChariot Test*» и сохранить копию экрана тестирования в файл. Для этого рекомендуется при активном окне «*IxChariot Test*» нажать комбинацию клавиш [*Alt*] - [*PrintScreen*], и после этого вставить изображение в документ *Microsoft Office Word* или в окно редактора *Paint*.

4) После проведения тестирования активировать закладку *Response Time* окна «*IxChariot Test*» и сохранить копию экрана тестирования в файл.

5) Выполнить отключение от точки доступа, для этого в окне беспроводного сетевого соединения операционной системы *Windows XP* активировать соединение с именем *AP*, и нажать на кнопку «Разъединить», как показано на рис. 4.9.

5. СОДЕРЖАНИЕ ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ

5.1. На основании исследований по п. 1.4.2. представить результаты исследований в виде таблицы по форме табл. 5.1.

Таблица 5.1 — Энергетические и информационные характеристики точек доступа

MAC адрес	Идентификатор сети	Частот- ный ка- нал	Рабо- чая частота	Ско- рость переда- чи, Мбит/с	Уровень мощно- сти, дБм	Отношение мощности сигнала к мощности шума, дБ

5.2. Для вариантов (Б — Г, Б — Д, В — Г, В — Д) произвести оценку расстояния до аппаратного роутера *DIR-400* (установленного вне аудитории

Б401), предполагая, что уровень мощности роутеров одинаков. Для получения оценки использовать измеренные уровни мощности используемого в лабораторной работе оборудования.

5.3. В отчете привести значения минимально, максимального и среднего времени отклика.

Таблица 5.2 — Временные характеристики для устройств *Wi-Fi* сети

Идентификатор сети	<i>IP</i> адрес	Вариант используемого протокола 802.11	Минимальное значение времени отклика, мс	Максимальное значение времени отклика, мс	Среднее значение времени отклика, мс

5.4. На основании исследований по п. 4.3. представить результаты исследований в виде таблицы по форме табл. 5.3. и по форме табл. 5.4.

Таблица 5.3 — Информационные характеристики устройств *Wi-Fi* сети

Идентификатор сети	<i>IP</i> адрес точки доступа	Вариант используемого протокола 802.11	Потенциальная скорость передачи, Мбит/с	Минимальное значение скорости передачи, Мбит/с	Максимальное значение скорости передачи, Мбит/с	Среднее значение скорости передачи, Мбит/с
	192.168.1.2					
	192.168.20.1					
	192.168.0.11					

Таблица 5.4 — Временные характеристики для устройств *Wi-Fi* сети

Идентификатор сети	<i>IP</i> адрес точки доступа	Минимальное значение времени отклика, мс	Максимальное значение времени отклика, мс	Среднее значение времени отклика, мс	Время тестирования, с
	192.168.1.2				
	192.168.20.1				
	192.168.0.11				

5.5. Для вариантов Б и В выполнить письменное обоснование результатов эксперимента при взаимной замене *IP* адресов точек сети.

5.6. Изобразить в отчете векторные диаграммы сигналов для используемых видов модуляции.

5.7. Представить в отчете структурную схему лабораторного стенда (см. рис.3.1) и показать на ней пути прохождения трафика по заданным вариантам (А, Б, В, Г, Д).

5.8. Сделать развернутые выводы, в которых отразить особенности полученных результатов для всех этапов исследования. В том числе:

— привести максимально подробную характеристику исследуемых в работе точек доступа (тип оборудования, частотный канал, вид шифрования данных, поддерживаемые скорости передачи информации;

— охарактеризовать полученные значения производительности с точки зрения потенциальных значений;

— указать причины отличия временных задержек при выполнении различных этапов эксперимента по п. 5.3.

6. КОНТРОЛЬНЫЕ ВОПРОСЫ

6.1. Вопросы для допуска к выполнению лабораторной работы

1) Поясните, в чем заключаются два режима работы сети стандарта *IEEE 802.11*.

2) Какие элементы лабораторной установки обеспечивают работу беспроводной сети стандарта *IEEE 802.11*?

3) Поясните, каким образом в беспроводных протоколах семейства 802.11 реализуется расширения спектра, и изобразите примерный вид спектров для исходного и преобразованного сигналов при использовании данного метода.

4) Изобразите простейшую структуру сети, на которой можно проиллюстрировать применение ПО *Chariot*, и укажите места установки необходимых программных модулей.

5) Какие подготовительные операции необходимо выполнить для тестирования *Wi-Fi* сети с помощью ПО *Chariot*?

6) Какие характеристики сети могут быть исследованы с помощью ПО *Chariot*?

7) В каком случае используется команда *ping*? Какие результаты она предоставляет? Приведите примеры команды *ping*.

8) Охарактеризуйте основные характеристики беспроводных сетевых устройств, которые могут быть получены с помощью программы *Netstumbler*.

9) Каким образом можно определить *IP* адрес компьютера при сетевом подключении?

10) Какие действия необходимо выполнить при подключении к сети *Wi-Fi* с помощью беспроводного сетевого соединения операционной системы *Windows*?

11) Охарактеризуйте порядок исследований в ходе выполнения лабораторной работы.

12) По какой причине могут отличаться результаты исследований, выполненных по вариантам соединений Б и Г (см. рис. 3.1)?

13) Пропускная способность какого порядка может быть получена при выполнении экспериментального исследования по вариантам соединений А и Б?

6.2. Вопросы для защиты лабораторной работы

1) Поясните, причины отличия уровней сигнала при исследовании различных точек доступа.

2) Поясните подробно, причины отличия пропускной способности при использовании различных точек доступа.

3) Поясните подробно, причины отличия времени отклика при использовании различных точек доступа.

4) Объясните, зачем в стандарте 802.11b предусмотрена скорость 5,5 Мбит/с, если при использовании ССК последовательностей можно передавать данные на скорости 11 Мбит/с.

5) Объясните, в чем заключается принцип реализации метода ортогонального частотного разделения с мультиплексированием *OFDM*. За счет чего при использовании метода *OFDM* происходит уменьшение влияния межсимвольной интерференции?

6) Объясните физические принципы реализации модуляции *DBPSK* и *DQPSK*.

7) Объясните физические принципы реализации модуляции *BPSK* и *QPSK*.

8) Объясните физические принципы реализации модуляции 16-QAM и 64-QAM.

9) Какие меры, помимо *WEP*, *WPA*, *WPA2*, могут использоваться в *Wi-Fi* оборудовании дополнительно для защиты передаваемых данных ?

10) Охарактеризуйте вид частотного плана для оборудования стандарта 802.11. Объясните, в чем заключаются причины ограничения количество одновременно близко расположенных работающих беспроводных устройств.

11) Поясните методику расчета расстояния до удаленной точки доступа *AP* и полученные результаты.

12) Охарактеризуйте полученные результаты производительности и временных задержек для различных точек доступа.

13) Охарактеризуйте уровни модели взаимодействия открытых систем, на которых работают протоколы 802.11.

14) Для чего используются методы расширения спектра в стандартах 802.11? В каких вариантах они реализуются?

15) Приведите порядок настройки беспроводного адаптера в режиме с закрытым идентификатором сети (*SSID*) на уровне характеристики основных этапов настройки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гейер, Д. Беспроводные сети. Первый шаг / Д. Гейер. — М.: Издательский дом «Вильямс», 2005. — 192 с.
2. Решение государственной комиссии по радиочастотам от 7 мая 2007 г., № 07-20-03-001. — Режим доступа: http://www.rfcmd.ru/sphider/docs/GKRCh/GKRCh_07-20-03-001_ot_07_05_2007.htm (дата обращения: 24.03.2019).
3. Рошан, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Рошан, Д. Лиэри. — М.: Издательский дом «Вильямс», 2004. — 304 с.
4. Роль коммуникационных протоколов и функциональное назначение основных типов оборудования корпоративных сетей // Н. Олифер, В. Олифер, Центр Информационных Технологий. — Режим доступа: <http://www.citforum.ru/nets/protocols/index.shtml> (дата обращения: 24.03.2019).
5. Чернега, В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.
6. Как работают протоколы *IEEE 802.11x* (общее техническое описание) / О.М. Гришанович. — Режим доступа: http://wifi.by.ru/info_protocols.htm (дата обращения: 24.03.2019).
7. Пахомов, С. Беспроводной маршрутизатор ASUS WL-566gM с поддержкой технологии *MIMO* / С. Пахомов // КомпьютерПресс. — 2006. — №5. — Режим доступа: <http://www.compress.ru/article.aspx?id=16399&iid=750> (дата обращения: 24.03.2019).

Приложение А — Нумерация каналов и частоты стандартов
IEEE 802.11 a/b/g/n

Стандарт *IEEE 802.11 b/g/n*

Номер канала	Частота, ГГц
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,468
13	2,472
14	2,484

Стандарт *IEEE 802.11 a/h/j/n*

Номер канала	Частота, ГГц
34	5,170
36	5,180
38	5,190
40	5,200
42	5,210
44	5,220
46	5,230
48	5,240
52	5,260
56	5,280
60	5,300
64	5,320
100	5,500
104	5,520
108	5,540
112	5,560
116	5,580
120	5,600
124	5,620
128	5,640
132	5,660
136	5,680
140	5,700
147	5,735
149	5,745
151	5,755
153	5,765
155	5,775
157	5,785
159	5,795
161	5,805
163	5,815
165	5,825
167	5,835
171	5,855
173	5,865
177	5,885
180	5,905

**ИССЛЕДОВАНИЕ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ
СТАНДАРТА *IEEE* 802.11b/g/n**

Учебно-методическое пособие

Составитель: Савочкин Александр Анатольевич

Издается в авторской редакции

Изд. № 238/19. Объем 2 п.л.
РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»