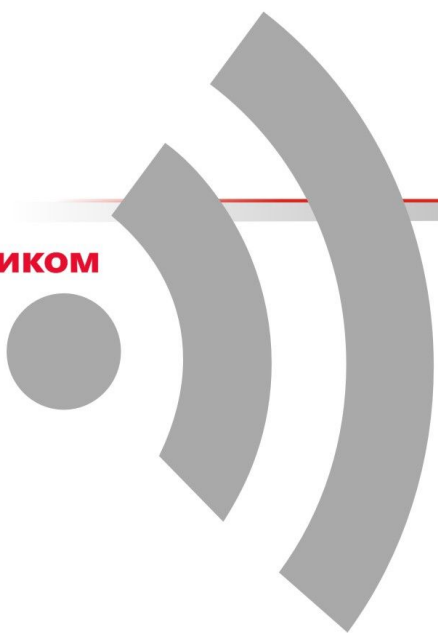


WWW.RUSMONITOR.RU

РИКОМ



ЗОДИАК

комплекс мониторинга беспроводных сетей

РУКОВОДСТВО ОПЕРАТОРА

версия 3.3.5

Оглавление

1 Введение.....	5
1.1 Назначение.....	5
1.2 Условные обозначения.....	5
1.3 Состав комплекса.....	5
1.4 Общие указания.....	6
1.5 Лицензионное соглашение.....	6
1.5.1 Лицензионный договор. Простая (неисключительная) лицензия.....	6
1.5.2 Техническая поддержка.....	7
2 Системные действия.....	9
2.1 Системные требования.....	9
2.2 Установка программы.....	9
2.3 Установка обновления версии программы.....	15
2.4 Удаление программы.....	15
2.5 Описание версий программы.....	16
3 Подготовка комплекса к работе.....	18
3.1 Подготовка аппаратной части.....	18
3.2 Запуск программы.....	18
4 Основные элементы интерфейса.....	20
4.1 Рабочее пространство.....	20
4.2 Главное меню.....	20
4.2.1 Файл.....	20
4.2.2 Действия.....	21
4.2.3 Настройки.....	21
4.2.4 Инструменты.....	21
4.2.5 Интерфейс.....	22
4.2.6 Окна.....	22
4.2.7 Помощь.....	23
4.3 Панель инструментов.....	23
4.4 Окна.....	24
4.4.1 Рабочие окна.....	24
4.4.2 Сервисные окна.....	25
4.5 Строка состояний.....	25
5 Работа с программой.....	27
5.1 Подключение приемника.....	27
5.2 Параметры.....	29
5.2.1 Общие.....	29
5.2.2 Обзорщик сети.....	31
5.3 Создание нового проекта.....	31
5.4 Открытие проекта из внешнего файла.....	32
5.5 Сохранение проекта во внешний файл.....	35
5.6 Запуск и остановка режима сканирования.....	37
5.7 Выбор языка.....	37
6 Окна.....	38
6.1 Окно Устройства WiFi.....	38
6.2 Работа со списком в окне Устройства WiFi.....	42
6.2.1 Выделение устройства в списке.....	42
6.2.2 Группировка списка.....	42
6.2.3 Сортировка списка.....	42

6.2.4	Изменение набора полей.....	43
6.2.5	Изменение положения и размера полей	45
6.2.6	Редактирование имени клиента.....	46
6.2.7	Навигация в окне Устройства WiFi.....	47
6.2.8	Изменение флага устройства.....	47
6.2.9	Скрытие устройств в списке.....	48
6.2.10	Удаление устройства из списка.....	48
6.3	Окно Связи WiFi.....	50
6.4	Работа со списком в окне Связи WiFi	51
6.4.1	Выделение соединений в списке.....	51
6.4.2	Группировка списка.....	52
6.4.3	Сортировка списка.....	52
6.4.4	Изменение набора полей.....	53
6.4.5	Изменение положения и размера полей списка.....	53
6.4.6	Навигация в списке.....	53
6.4.7	Изменение флага соединения.....	54
6.4.8	Скрытие соединений в списке.....	54
6.4.9	Удаление соединения из списка.....	54
6.4.10	Запись истории соединения.....	54
6.5	Окно Устройства Bluetooth.....	56
6.6	Работа со списком в окне Устройства Bluetooth.....	58
6.6.1	Сортировка списка.....	58
6.6.2	Изменение набора полей.....	58
6.6.3	Изменение положения и размера полей.....	58
6.6.4	Навигация в списке.....	58
6.6.5	Изменение флага устройства.....	58
6.6.6	Скрытие устройства в списке.....	58
6.6.7	Удаление устройства из списка.....	58
6.7	Окно Устройства ZigBee.....	59
6.8	Работа со списком в окне Устройства ZigBee.....	61
6.8.1	Сортировка списка.....	61
6.8.2	Изменение набора полей.....	61
6.8.3	Изменение положения и размера полей.....	61
6.8.4	Навигация в списке.....	61
6.8.5	Изменение флага устройства.....	61
6.8.6	Скрытие устройства в списке.....	61
6.8.7	Удаление устройства из списка.....	61
7	Окно Граф.....	62
7.1	Назначение режима графа.....	62
7.2	Переход в режим графа.....	62
7.3	Внешний вид и описание окна графа.....	62
8	Окно Монитор.....	65
8.1	Назначение режима монитора.....	65
8.2	Переход в режим монитора.....	65
8.3	Внешний вид и описание окна монитора.....	65
9	Правила.....	70
9.1	Назначение правил	70
9.2	Окно Правила.....	71
9.3	Структура дерева правил.....	72

9.4 Создание правила.....	73
9.5 Выбор условий Правила.....	73
9.5.1 Область ввода условий для устройств WiFi.....	73
9.5.2 Область ввода условий для соединений WiFi.....	76
9.5.3 Область ввода условий для устройств Bluetooth.....	81
9.5.4 Область ввода условий для устройств ZigBee.....	81
9.6 Выбор действий для Правил.....	82
9.7 Работа с правилами в режиме сканирования.....	84
10 Поиск «невидимых» устройств Bluetooth.....	85
11 Отчет.....	87
12 Методические рекомендации.....	89
12.1 Полезные советы.....	89
13 Паспорт.....	90

1 Введение

1.1 Назначение

Настоящая программная оболочка является специальным программным обеспечением (далее программа) комплекса радиоконтроля беспроводных сетей ЗОДИАК (далее комплекс). Комплекс предназначен для мониторинга диапазонов частот 2.4 и 5 ГГц* и обнаружения устройств, использующих беспроводные стандарты WiFi, Bluetooth и ZigBee для передачи негласно полученной информации, а так же позволяет контролировать WiFi устройства, в том числе, и за пределами зоны радиовидимости.

Комплекс имеет специализированный интерфейс в виде структурированных списков устройств и их связей. Интерфейс специально разрабатывался для оптимального представления информации о устройствах беспроводных сетей. Комплекс оснащен набором специализированных инструментов для автоматической классификации опасных признаков и нестандартных сочетаний параметров клиентов сетей. Работа с комплексом не требует специальной подготовки оператора в области администрирования сетей, поскольку интерфейс комплекса оптимизирован и интуитивно понятен для специалистов знакомых с системами радиомониторинга и радиоконтроля. ЗОДИАК может одинаково эффективно применяться как для проведения спецобследований помещений, так и для стационарного радиомониторинга объекта.

1.2 Условные обозначения



ВНИМАНИЕ. Этот пункт содержит информацию, которая может оказаться критичной для целостности пользовательской информации или работоспособности комплекса в целом.



ПРИМЕЧАНИЕ. Этот пункт дополняет или разъясняет информацию содержащуюся в соответствующей главе.



СОВЕТ. Этот пункт содержит полезные советы по использованию режимов или инструментов программы.

1.3 Состав комплекса

Комплекс состоит из приемника, программы и набора беспроводных адаптеров, состав которого может изменяться в зависимости от

* Диапазон рабочих частот зависит от комплектации комплекса.

поставляемой конфигурации. С комплектом поставляются следующие адаптеры:

- WiFi адаптер;
- Bluetooth адаптер*;
- ZigBee pro адаптер*.

В состав комплекта может входить управляющая ПЭВМ* к которой подключается приемник и на которую устанавливается программа.

При поставке управляющей ПЭВМ программа поставляется предустановленной.

1.4 Общие указания

Все программное обеспечение и драйвера, которые необходимы для работы приемника полностью сконфигурированы производителем для начала работы. Никакие дополнительные настройки аппаратной части приемника со стороны оператора не требуются.



Не допускается самостоятельная замена и/или модернизация пользователем аппаратной части и/или операционной системы приемника.

1.5 Лицензионное соглашение

1.5.1 Лицензионный договор. Простая (неисключительная) лицензия

ООО «РИКОМ» (далее Лицензиар), являясь обладателем исключительного права на использование программного обеспечения «ЗОДИАК» (далее программа), предоставляет Лицензиату право использования экземпляра программы в пределах права использования 1 (одной) копии программы на вычислительном средстве, входящем в комплект автоматизированного комплекса радиоконтроля «ЗОДИАК» (далее комплекс), в пределах возможностей версии программы, которые указаны в руководстве оператора.

Вознаграждение за использование экземпляра программы входит в стоимость программы.

Передача Лицензиатом третьим лицам права на использование экземпляра программы, полученного в рамках настоящей лицензии, может быть совершена исключительно с письменного согласия Лицензиара.

Лицензиат не имеет права распространять программу в любой форме. Под распространением понимается предоставление доступа третьим лицам к программе любым способом отчуждения.

В случае нарушения (превышения) со стороны Лицензиата положений

* Поставляется дополнительно

настоящей Лицензии Лицензиар, на основании ст. 1252 ч.4 Гражданского кодекса РФ, имеет право на защиту исключительных прав путем предъявления требования:

1 - о признании права - к лицу, которое отрицает или иным образом не признает право, нарушая тем самым интересы правообладателя;

2 - о пресечении действий, нарушающих право или создающих угрозу его нарушения - к лицу, совершающему такие действия или осуществляющему необходимые приготовления к ним;

3 - о возмещении убытков или выплате – к лицу, неправомерно использовавшему результат интеллектуальной деятельности без заключения соглашения с правообладателем (бездоговорное использование), либо иным образом нарушившему его исключительное право и причинившему ему ущерб;

4 - о приостановлении (прекращении) технической поддержки программы – к лицу допустившему бездоговорное использование.

Право использования экземпляра программы предоставляется с сохранением за Лицензиаром права выдачи лицензий другим лицам (простая (неисключительная) лицензия). Лицензиар сохраняет имущественное право на оригинал программы, а так же на все последующие экземпляры программы независимо от формы носителя, в котором существуют другие экземпляры. Авторские права на все экземпляры программы и сопроводительные материалы (на бумажных и электронных носителях) к нему защищены в соответствии с законодательством Российской Федерации. Компилирование программы, ее декомпилирование, модификация, а так же копирование сопроводительных документов, без письменного согласия со стороны Лицензиара, запрещено, за исключением случаев, когда осуществление указанных действий разрешено законодательством РФ. Программа не защищена от копирования, однако Лицензиат не имеет права делать копии с экземпляра программы.

Настоящая Лицензия, в случае согласия, выраженного в форме молчания в течение 7 дней с момента приобретения программы, в соответствии со ст. 443 ГК РФ имеет силу договора. В случае несогласия пользователя с условиями настоящей Лицензии, последний обязан в течение 7 (семи) дней с момента приобретения программы вернуть его по месту приобретения.

1.5.2 Техническая поддержка.

ООО «РИКОМ» - являясь разработчиком программы (далее – Разработчик) - гарантирует пользователям (далее - Пользователь), которые легально приобрели программу и соблюдают условия Лицензии следующие виды технической поддержки программы:

1 - бесплатные консультации по использованию программы;

2 - бесплатные модернизации данной версии программы в случае обнаружения ошибок, которые существенно влияют на работоспособность программы;

3 - платное дополнение текущей версии экземпляра программы опцией, которая расширяет возможности программы;

4 - платную модернизацию экземпляра программы и/или опций на новую версию.

Форма и порядок выпуска модернизаций определяются Разработчиком.

Настоящие гарантийные обязательства действительны:

1 - в отношении бесплатной модернизации – не менее чем в течение 1 года с момента выпуска версии программы или опции, при условии что Разработчик не объявил через свой сайт в Интернет о прекращении поддержки данной версии или опции;

2 - в отношении остальных модернизаций – в течение всего времени использования программы, при условии, что Разработчик не объявил через свой сайт в Интернет о прекращении продаж данной версии или опции.

В случае обнаружения дефектов носителей программы, Разработчик гарантирует их замену в течение 90 (девяносто) дней с момента приобретения, при условии легального приобретения программы и соблюдения требований Лицензии и если работоспособность носителя не нарушена в результате неправильного обращения.

Пользователь получает право на техническую поддержку программы с момента приобретения.

Разработчик имеет право приостановить техническую поддержку, если пользователь не ознакомился должным образом с настоящим руководством оператора.

Условия прекращения гарантийных обязательств и технической поддержки:

1 - несоблюдение требований Лицензии;

2 - несовпадение данных о фактическом пользователе программы и/или версии (опции) программы с регистрационными данными пользователя, которые находятся у Разработчика;

3 - неправильное использование программы в составе комплекса;

4 - самостоятельная замена и/или модернизация пользователем аппаратной части и/или операционной системы комплекса.

Информацию о текущей версии (подверсии) и об установленных опциях пользователь может получить в разделе « О программе» главного меню.

2 Системные действия

2.1 Системные требования.

Для нормальной работы программе необходимы следующие минимальные требования:

Операционная система: Windows 7 (x32 и x64).

Процессор: не хуже Core 2 Duo

Оперативная память: 1 ГБ

Место на жестком диске: 1 ГБ

2.2 Установка программы

Перед установкой программы, убедитесь, что программа уже не установлена. В противном случае, выполните процедуру удаления предыдущей версии программа и только после этого установку.

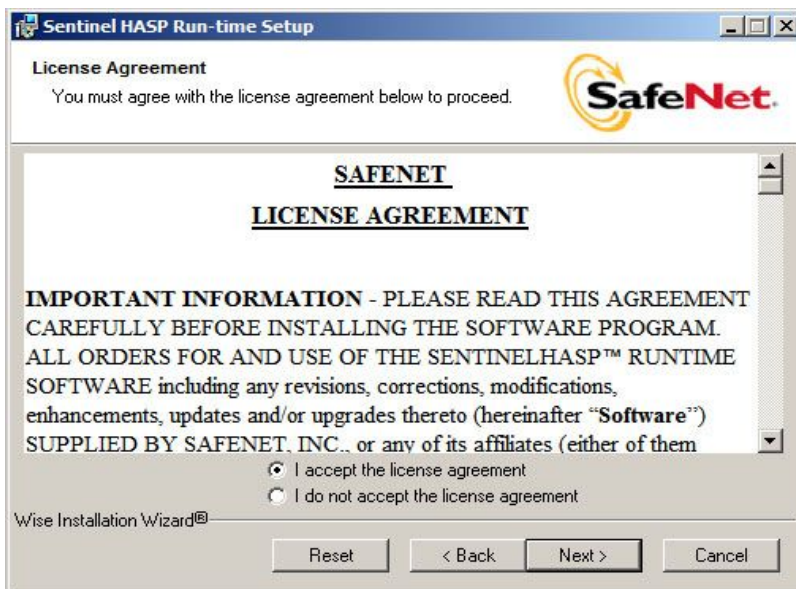
В первую очередь установите HASP ключ, для чего запустите HASPUserSetup.exe с установочного диска из комплекта поставки, перед этим убедитесь, что сам ключ не вставлен в ПЭВМ.

В начале установки появляется окно установщика:

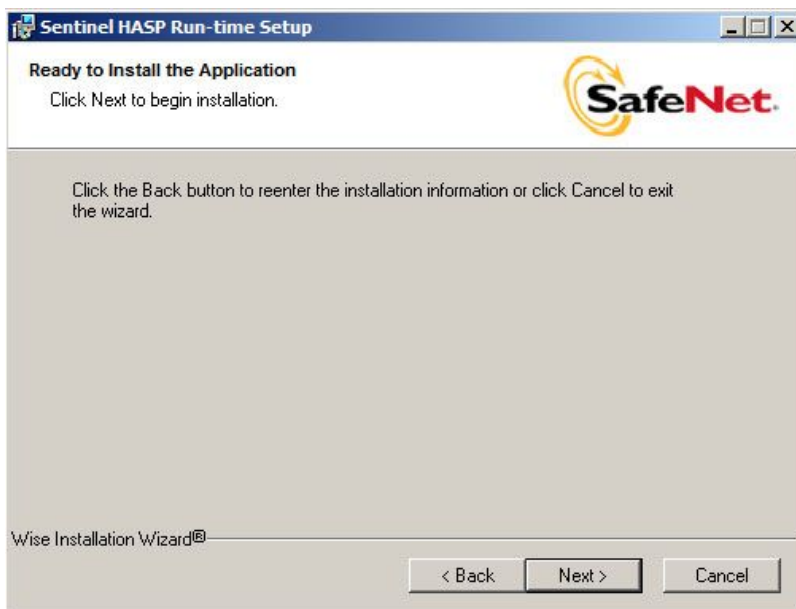


Для начала установки следует нажать «Next».

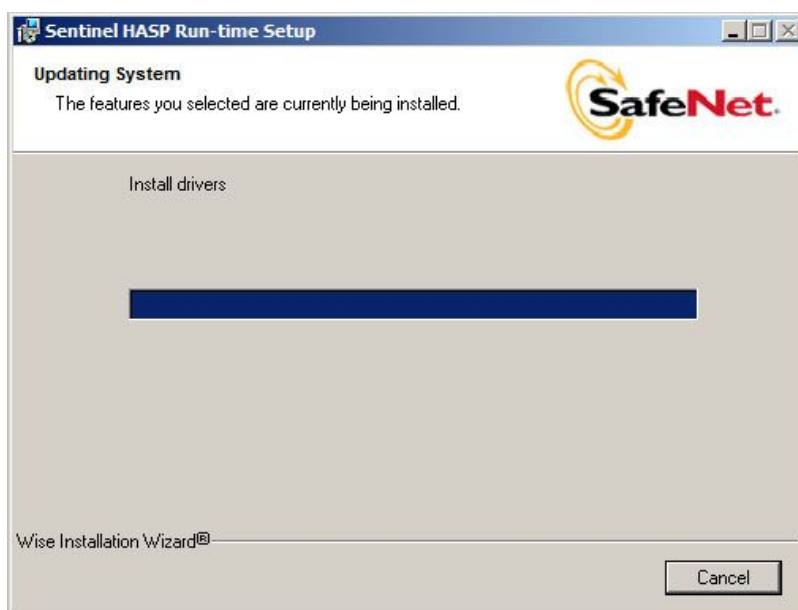
Далее следует ознакомиться с текстом лицензионного соглашения на программу, выбрать пункт «I accept the license agreement», нажать «Next» и установка будет продолжена.



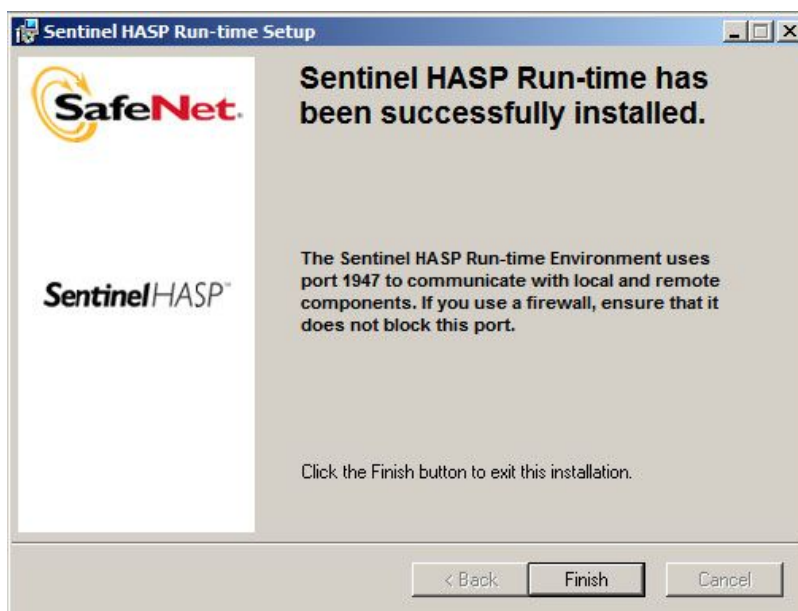
Далее появится окно подтверждения установки. Нажмите «Next» и установка будет продолжена.



Установка системы может занять несколько минут.



При удачно завершении установки появиться окно:



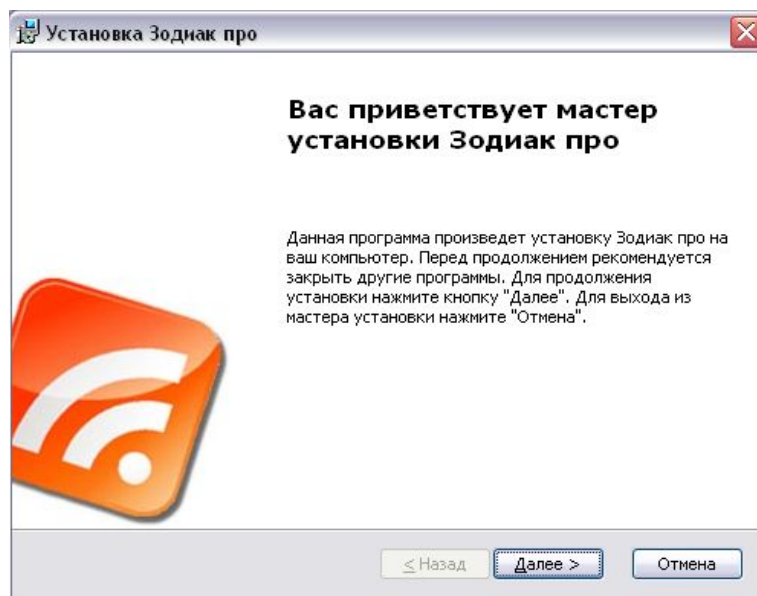
Нажмите «Finish». Вставьте HASP ключ в ПЭВМ, убедитесь, что на нем горит красный индикатор. В случае если световой индикации нет — выньте ключ и вставьте снова. Перейдите к установке программы.

Установка программы выполняется из дистрибутива в файле zodiac_pro_setup.msi



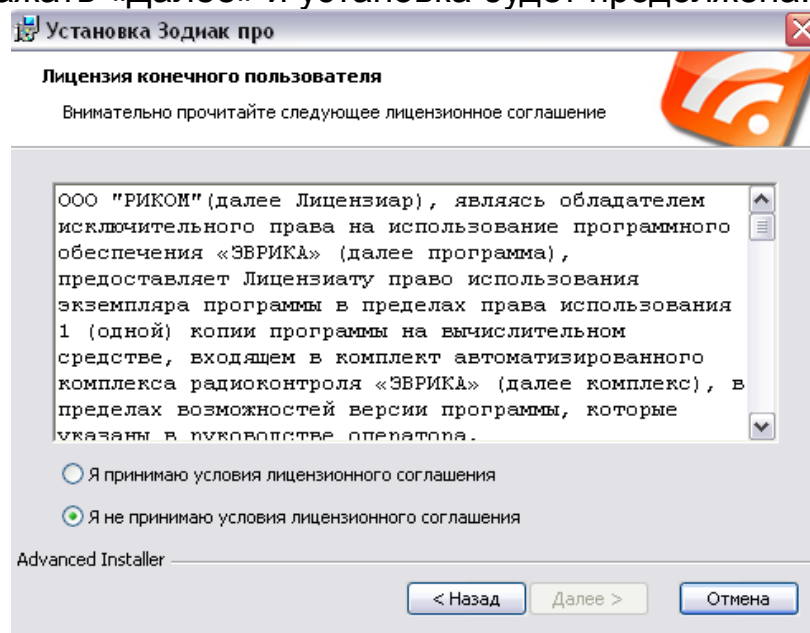
Программа поставляется с дистрибутивом для x32 и x64 операционных систем Windows. Тип системы указывается в названии файла установщика.

В начале установки появляется окно установщика программы:

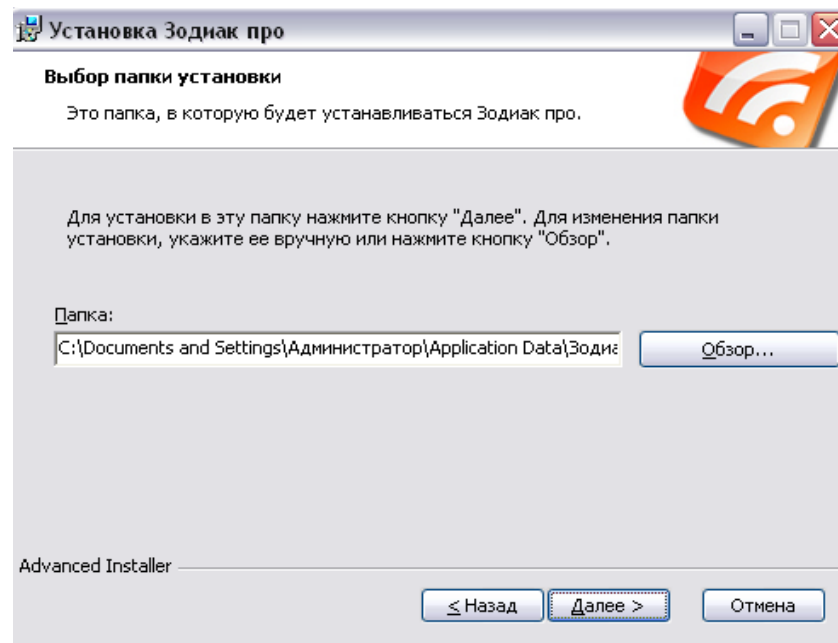


Для начала установки следует нажать «Далее».

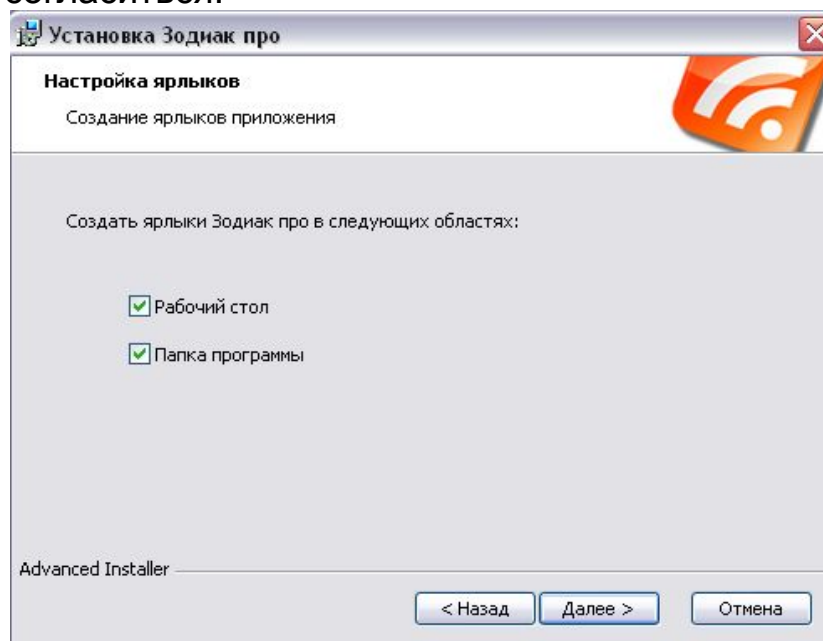
Далее следует ознакомиться с текстом лицензионного соглашения на программу, выбрать пункт «Я принимаю условия лицензионного соглашения», нажать «Далее» и установка будет продолжена.



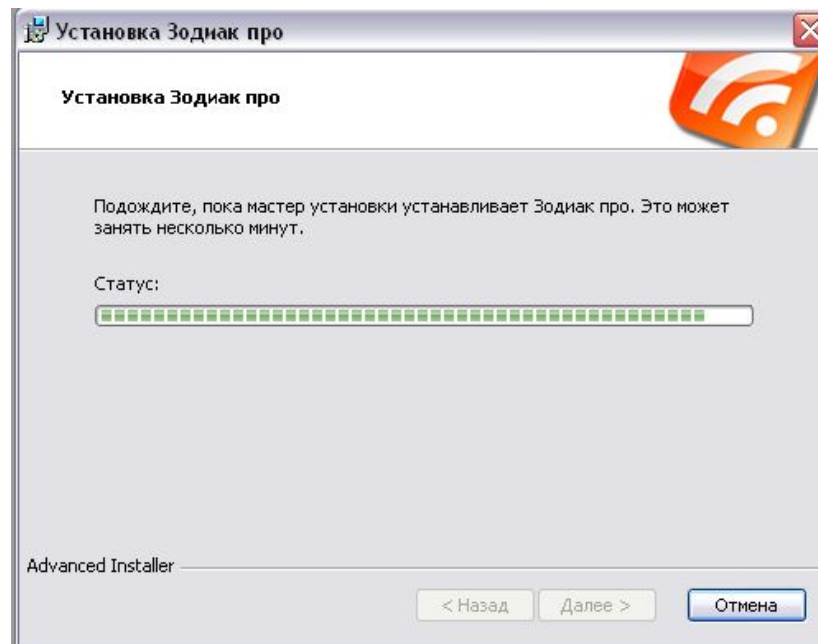
В следующем окне следует выбрать папку в которую будет установлена программа:



В следующем окне установщик предложит создать ярлыки программы, рекомендуется согласиться:



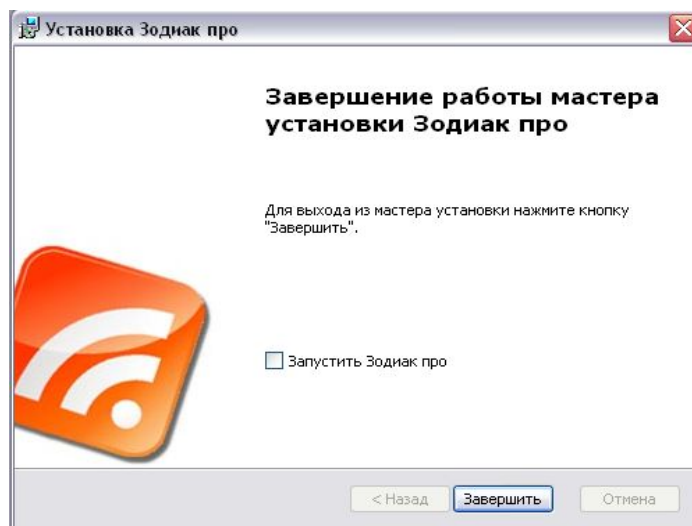
На этом предварительные настройки закончены, программа сообщит о готовности к установке, для продолжения следует нажать «Далее». Процесс установки отображается в рабочем окне:



После установки драйвера ключа HASP программа выдаст сообщение:



Необходимо нажать Ок для завершения установки.
При удачно завершении установки появиться окно:



После нажатия «Завершить», если установка производилась с настройками по умолчанию, в меню Пуск\Программы\Зодиак про появятся ярлыки Программы, Руководства пользователя (в формате Adobe Acrobat) и Деинсталлятора программы.

При первом подключении ключа операционная система может потребовать повторно установить драйвер, в этом случае необходимо установить драйвер следуя указанием системы.

2.3 Установка обновления версии программы

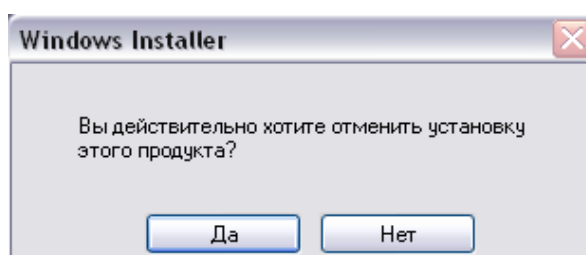


При установке обновленной версии программы необходимо удалить конфигурационные файлы старой версии. Свяжитесь с разработчиком для получения пути по которому располагаются конфигурационные файлы и инструкции по модернизации оболочки.

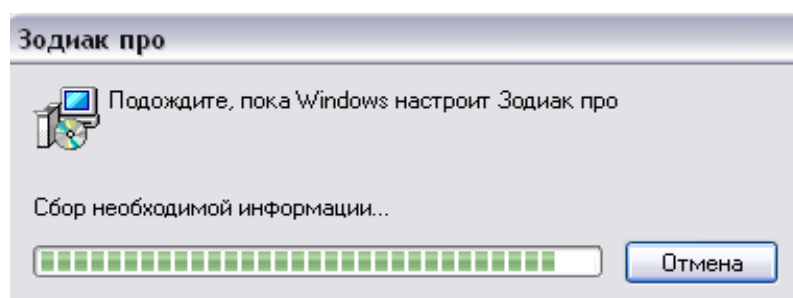
2.4 Удаление программы

Для удаление программы необходимо выбрать пункт «Удаление программы» в меню Пуск\Программы\Зодиак про.

Программа запросит подтверждение процедуры удаления:



Для удаления программы следует нажать «Да». Процесс удаления отображается в рабочем окне Windows Installer:



В процессе удаления возможно появление информационного окна драйвера HASP ключа. В нем следует нажать Ок после чего удаление программы будет продолжено.

По окончании удаления информационное окно Windows Installer пропадет.

2.5 Описание версий программы

Версии программы нумеруются двумя числами, разделенными точкой, например, ЗОДИАК 3.1. Первое число (3) характеризует версию программы, второе - релиз данной версии.

Приобретая ЗОДИАК, Пользователь получает бесплатную поддержку всех релизов, приобретаемой версии.

Существуют также две модификации программы: «про» и «сетевая» различающиеся набором функций.

Просмотреть сведения о текущей версии программы можно в окне «О программе», выбрав пункт главного меню Помощь — О программе, представленное на рисунке 1.

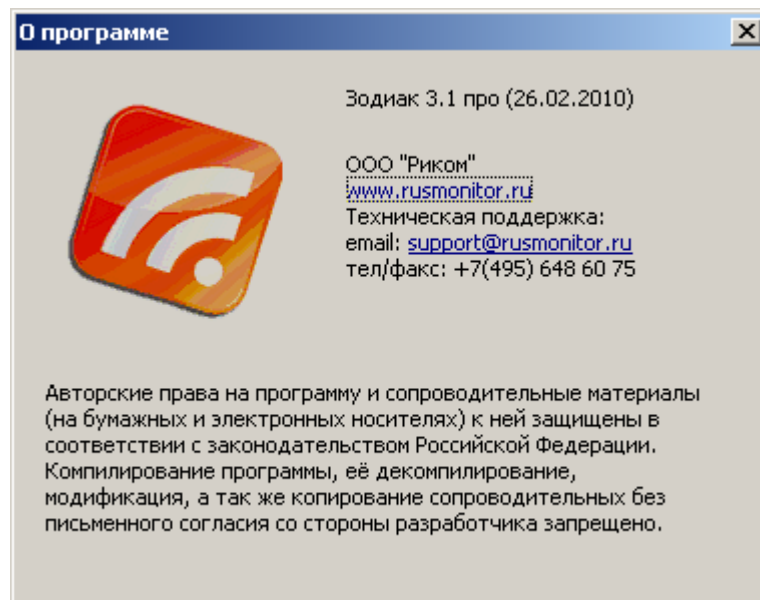


Рисунок 1 - Внешний вид окна О программе

В этом окне также указывается дата выхода релиза и уникальный номер комплекса, позволяющий идентифицировать пользователя продукта.



Всегда сообщайте номер комплекса при обращении в службу технической поддержки.

3 Подготовка комплекса к работе

3.1 Подготовка аппаратной части

- Достаньте приемник из упаковки.
- Если комплекс поставляется с USB адаптерами (WiFi, Bluetooth или ZigBee) - подключите адаптеры к приемнику.
- Подключите антенны к встроенному адаптеру WiFi.
- Подключите приемник к сети.
- Подключите приемник к управляющей ПЭВМ с помощью сетевого кабеля, который поставляется в комплекте с комплексом.



По умолчанию приемник сконфигурирован для подключения непосредственно к ПЭВМ с помощью патч-корда распаянного под кросс и не требует изменения сетевых настроек. При этом приемник имеет по умолчанию IP адрес 192.168.0.77, а ПЭВМ имеет IP адрес 192.168.0.2.


ВАЖНО, что бы приемник и ПЭВМ были в одной подсети, по умолчанию маска подсети 255.255.255.0.

Приемник так же может быть подключен к ПЭВМ и через сеть.


Если для такого подключения требуется сменить IP адрес приемника или установить DHCP- следует обратиться в техническую поддержку разработчика.

В случае, если приемник подключается не непосредственно к управляющей ПЭВМ, а через локальную сеть, то подключение приемника должно производиться патч-кордом распаянным 1:1.

После подключения приемник необходимо включить нажав на кнопку «сеть». Подтверждением включения приемника является загорание светового индикатора на приемнике. Через 20 секунд после включения, приемник готов к работе.

Выключение приемника производится нажатием на кнопку сеть, или программно из окна «Обозреватель сети» (**глава 5.1**) нажатием на кнопку , при этом будет осуществлено выключение помеченного галочкой, занятого программой приемника.

3.2 Запуск программы

Программа запускается с помощью ярлыка  с именем программы на рабочем столе или через меню кнопки «Пуск» ОС Windows.

При попытке запуска второй копии программы оператору выдается предупреждающее окно.

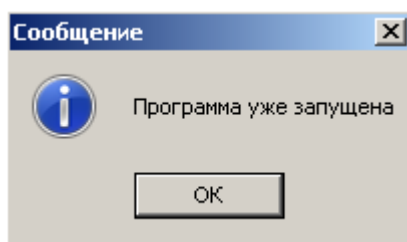


Рисунок 2- Предупреждающее окно

В случае сбоев в работе программы или ПЭВМ, следует немедленно обратиться в службу технической поддержки производителя.

При запуске программы откроется рабочее пространство программы и во все окна программы будет загружен текущий Проект.

Имя проекта отображается в шапке окна рабочего пространства программы, по умолчанию- «Новый проект».

4 Основные элементы интерфейса

4.1 Рабочее пространство

Рабочее пространство программы представлено на рисунке 3.

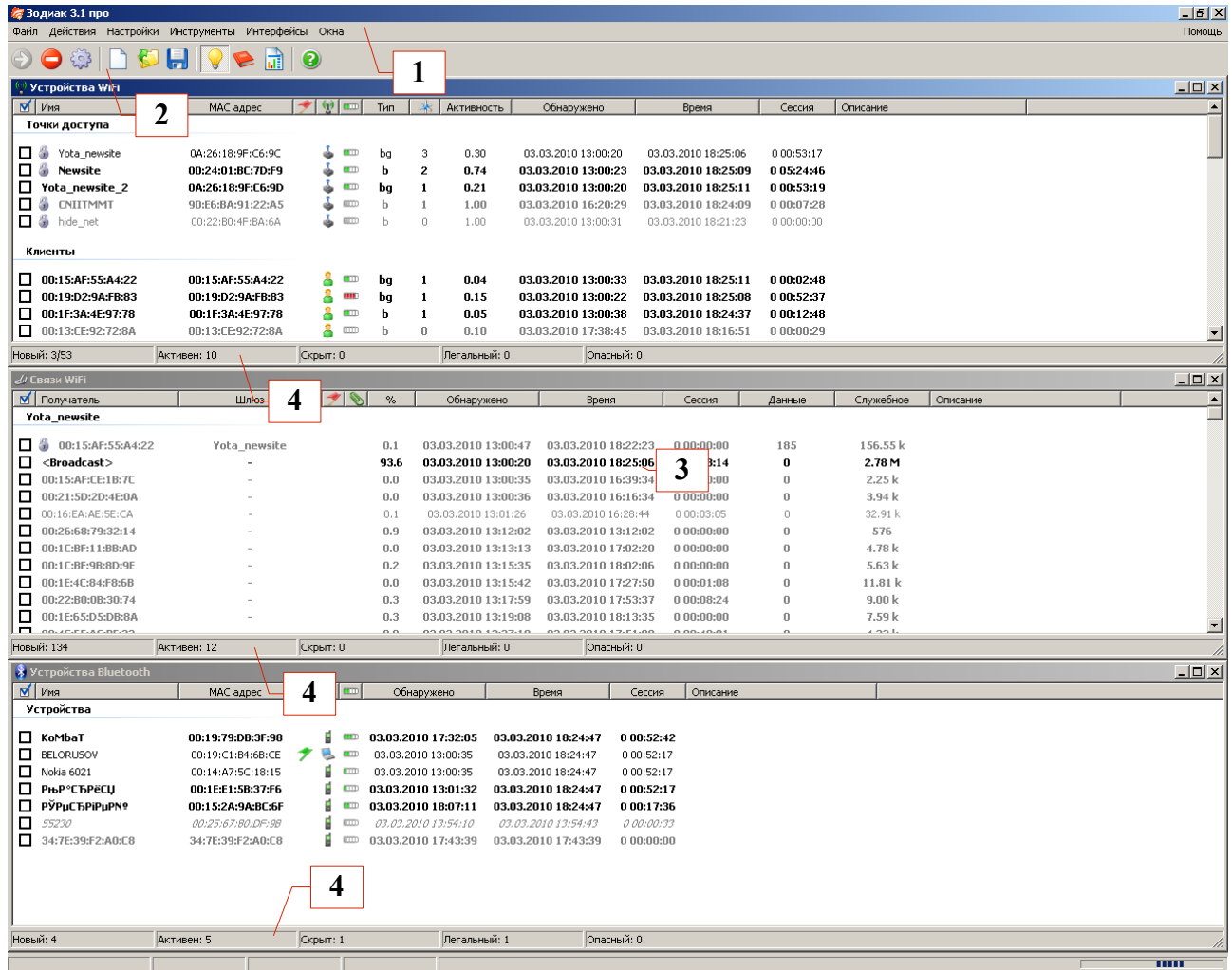


Рисунок 3 - Внешний вид рабочего пространства

Рабочее пространство состоит из:

- 1 - Главное меню.
- 2 - Панель инструментов.
- 3 - Рабочие окна и сервисные программы.
- 4 - Строка состояния.

4.2 Главное меню

4.2.1 Файл

Позволяет оператору работать с проектом. Описание пунктов меню «Файл» приведено в таблице 1.

Наименование	Описание
Новый проект	Создает новый проект
Открыть проект	Открывает проект из указанного пользователем файла
Сохранить проект	Сохраняет текущий проект в указанный пользователем файл
Выход	Завершает работу с программой

Таблица 1: Пункты меню «Файл»

4.2.2 Действия

Позволяет оператору запускать и останавливать работу программы. Описание пунктов меню «Действия» приведено в таблице 2.

Наименование	Описание
Начать сканирование	Запускает режим сканирования для всех режимов программы.
Остановить сканирование	Останавливает режим сканирования для всех режимов программы.

Таблица 2: Пункты меню «Действия»

4.2.3 Настройки

Позволяет оператору изменять настройки программы и аппаратной части комплекса. Описание пунктов меню «Настройки» приведено в таблице 3.

Наименование	Описание
Параметры	Позволяет менять настройки программы
Обозреватель сети	Позволяет подключать и отключать приемники, а так же изменять их настройки.

Таблица 3: Пункты меню «Настройки»

4.2.4 Инструменты

Позволяет оператору вызывать дополнительные инструменты для обработки и представления данных. Описание пунктов* меню «Инструменты» приведено в таблице 4.

Наименование	Описание
--------------	----------

* Пункты меню «Граф» и «Монитор» доступны только при активном окне «Устройства WiFi» / «Связи WiFi»

Правила	Вызывает окно для создания и редактирования правил.
Граф	Вызывает окно представления связей устройства в виде графа.
Монитор	Вызывает окно с столбиковой диаграммой передаваемого устройством трафика.
Отчет	Позволяет автоматически сформировать отчет.

Таблица 4: Пункты меню «Инструменты»

4.2.5 Интерфейс

Позволяет оператору включать и выключать рабочие окна. Описание пунктов меню «Инструменты» приведено в таблице 5.

Наименование	Описание
Устройства WiFi	Открывает/закрывает окно со списком обнаруженных устройств WiFi.
Связи WiFi	Открывает/закрывает окно со связями устройств WiFi, которые находятся в окне Устройства WiFi.
Устройства Bluetooth	Открывает/закрывает окно со списком обнаруженных устройств Bluetooth.

Таблица 5: Пункты меню «Интерфейс»

4.2.6 Окна

Позволяет оператору управлять с видом и расположением рабочих окон на рабочем пространстве. Описание пунктов меню «Окна» приведено в таблице 6.

В меню «Окна» также располагается перечень всех открытых рабочих окон. Активное окно выделено галочкой.

Наименование	Описание
Каскадом	Располагает рабочие окна каскадом. Активное окно всегда сверху.
Горизонтально	Располагает окна горизонтально. Активное окно всегда сверху
Вертикально	Располагает окна вертикально. Рабочее окно всегда слева.

Наименование	Описание
Заккрыть все	Закрывает все окна на рабочем пространстве.

Таблица 6: Пункты меню «Окна»

4.2.7 Помощь

Содержит справочную информацию «О программе» и настоящее руководство в электронном виде. Описание пунктов меню «Помощь» приведено в таблице 7.

Наименование	Описание
Справка	Открывает электронную версию руководства пользователя в формате pdf.
О программе	Позволяет оператору получить информацию о версии программы и серийном номере комплекса

Таблица 7: Пункты меню «Помощь»



Просмотр руководства пользователя в электронном виде осуществляется с помощью программы Adobe Acrobat Reader.

4.3 Панель инструментов

Панель инструментов программы расположена над окнами и состоит из кнопок.

Описание кнопок панели инструментов приведено в таблице 8.







Обозн.	Наименование	Описание	В меню
	Сканирование	Начинает сканирование	Действия-Начать сканирование
	Стоп	Останавливает сканирование	Действия-Остановить сканирование
	Параметры	Открывает окно настроек программной оболочки	Действия -Параметры
	Обозреватель сети	Открывает окно обозревателя сети	Действия -Обозреватель сети
	Новый проект	Создает новый проект	Файл -Новый проект
	Открыть проект	Открывает проект из указанного пользователем файла	Файл -Открыть проект
	Сохранить проект	Сохраняет текущий проект в указанный пользователем файл	Файл -Сохранить проект
 	Показать скрытые	Показывает/скрывает скрытые пользователем, системой или правилами устройства и соединения.	нет
	Правила	Открывает окно правил для создания и редактирования	Инструменты - Правила
	Отчет	Создает отчет о работе	Инструменты - Отчет
	Помощь	Открывает руководство пользователя	Помощь-Справка


Таблица 8: Кнопки инструментальной панели главного окна

4.4 Окна

4.4.1 Рабочие окна

•Окно «Устройства WiFi». Обозначается иконкой  . Отображает список обнаруженных устройств WiFi.

•Окно «Соединения». Обозначается иконкой  . Отображает список обнаруженных соединений для устройств WiFi.

•Окно «Устройства Bluetooth». Обозначается иконкой  . Отображает список обнаруженных устройств Bluetooth.

Очень важной особенностью рабочих окон является возможность списков автоматически классифицировать объекты по степени актуальности:

Новые -это устройства или соединения, которые попали в базу данных


при текущем цикле сканирования в первый раз - строка в списке выделяется жирным шрифтом


Не новые — строка в списке без выделения жирным.

Активные- это устройства или соединения которые обнаруживаются комплексом при текущем сканировании или были обнаружены ранее, но в пределах «интервала неактивности» заданного в настройках — строка в списке черным цветом


Не активные — строка в списке серым цветом и менее контрастными значками.


Соответственно, список может отображать и все возможные сочетания актуальности сигналов, например Новые и неактивные — жирным шрифтом, серым цветом.

•Окно «Граф». Обозначается иконкой . Окно предназначено для визуального анализа соединений выбранного WiFi устройства.

•Окно «Монитор». Обозначается иконкой . Окно предназначено для контроля трафика управления и данных для выбранного соединения.

4.4.2 Сервисные окна

•Окно «Параметры». Обозначается иконкой . Отображает общие настройки программной оболочки

•Окно «Правила». Обозначается иконкой . Отображает список правил фильтрации устройств и соединений по разведпризнакам и служит для создания и редактирования пользовательских правил фильтрации устройств и их соединений.



Сервисные окна не упорядочиваются и не закрываются с помощью инструментов пункта главного меню «Окна».

4.5 Строка состояний

Внешний вид строки состояний рабочего окна представлен на рисунке 4.



Рисунок 4: Строка состояний рабочего окна

Строка состояния отображает количество обнаруженных объектов для выбранного режима- WiFi или Bluetooth.

В строке состояний приведена информация об общем количестве обнаруженных устройств WiFi и Bluetooth.

Внешний вид строки состояний рабочего окна представлен на рисунке 5.



Рисунок 5: Строка состояний главного окна

В правом нижнем углу строки состояния отображается значок процесса сканирования. Значок отображается только при включенном сканировании.

5 Работа с программой

5.1 Подключение приемника

Комплекс поставляется с сконфигурированным сетевым интерфейсом приемника. Для того, что бы убедиться, что приемник подключен корректно и с ним есть связь, необходимо запустить окно сетевого обозревателя из главного меню Настройки-Обозреватель сети. Внешний вид окна обозревателя представлен на рис.6

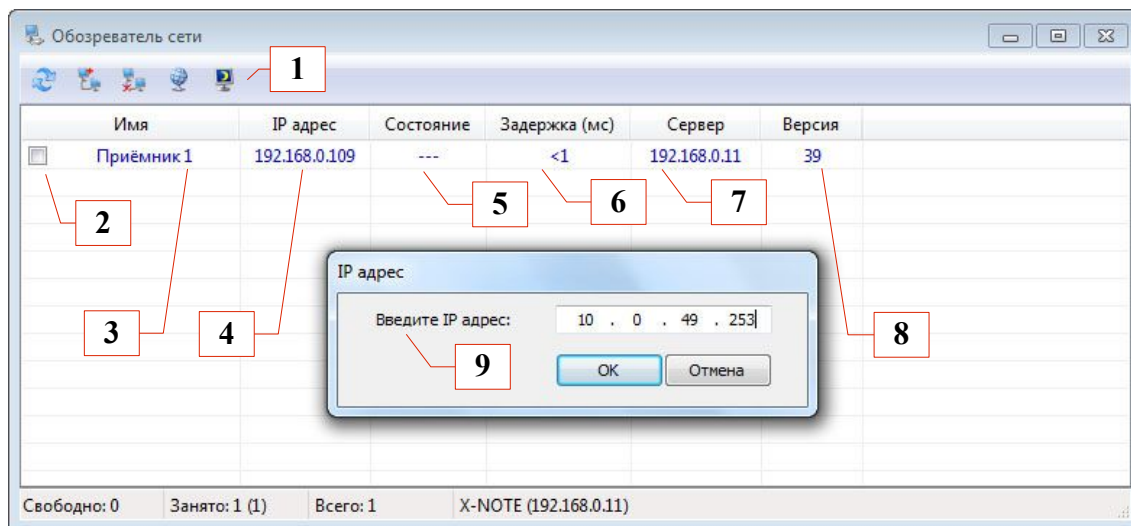


Рисунок 6: Внешний вид окна Обозреватель сети

Окно обозревателя состоит из:

1- Панель инструментов (кнопки):

–«обновить»;

–«занять»;

–«освободить приемники»;

–«подключение приемника по IP адресу»;

–«выключение приемника».

2- Поле выбор

3- Имя -поле сетевым именем приемника

4- IP адрес - поле с сетевым адресом приемника

5- Состояние - отображается типы адаптеров, которые подключены к приемнику:

W- адаптер WiFi

B- адаптер Bluetooth.

Z- адаптер ZigBee.

Отображение состояния маленькими буквами означает что адаптер доступен, отображение большими буквами обозначает, что адаптер активен

и программа собирает с него данные.

6- Задержка. Определяет задержку при прохождении пакетов от приемника к программе. Задержка менее 100 мс считается удовлетворительной для нормальной работы комплекса.

7- Сервер- IP адрес компьютера с программой которой занят этот приемник.

8- Номер версии программы приемника.

Для подключения приемника необходимо нажать кнопку «обновить», и, в случае успешного установления связи, приемник будет отображен в списке.



Кнопка «Обновить» отобразит приемники только если они находятся в одной подсети с управляющей ПЭВМ. В противном случае для подключения следует воспользоваться подключением по IP адресу.

Если приемник отображен синим цветом значит он подключен и готов к работе.


Если приемник отображен зеленым цветом, значит он готов к подключению. Подключить приемник можно выбрав его в списке в поле выбор и нажав кнопку «занять». После подключения приемник изменит цвет на синий.



В списке может быть несколько доступных для подключения приемников, но занять можно только один, любой.

Если приемник отображен серым цветом значит он уже занят другой программой и временно недоступен для подключения.

Что бы занять другой приемник, необходимо сначала, выбрать из списка в поле выбор, уже занятый приемник и освободить его, нажав кнопку «освободить приемники».

Также приемник можно подключить зная его IP адрес, например если приемник находится в другой подсети, для чего нажмите кнопку  , в появившемся диалоговом окне (9) укажите его IP и нажмите «ОК».

Пока приемник не занят кнопка начала сканирования в программе будет недоступной.

Если в процессе работы комплекса связь с приемником, по каким-либо причинам потеряна, оператор будет проинформирован об этом факте сообщением:

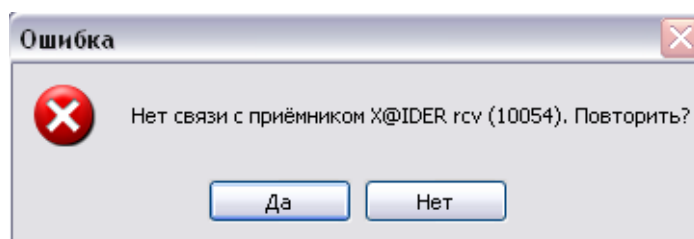


Рисунок 7: Ошибка связи с приемником

При нажатии Да, программа повторит поиск приемника с установленными ранее параметрами и при нахождении, автоматически подключит приемник без участия оператора.

Информация о подключенном приемнике автоматически сохраняется программой при выходе из нее. При повторном запуске программы, подключенный ранее приемник будет подключен автоматически.




Если в момент открытия программы подключенный ранее приемник был выключен, то его подключение будет аннулировано. В этом случае, после выхода и повторного старта программы потребуется подключить приемник снова.

Приемник может быть выключен из программы кнопкой «выключение приемника». Комбинация Cntrl+кнопка «выключение приемника» приведет к его перезагрузке.

5.2 Параметры

5.2.1 Общие

Окно конфигурации параметров программы вызывается с помощью кнопки  на панели инструментов или из Главного меню Настройки-Параметры.

Окно настроек программы представлено на рисунке 8.

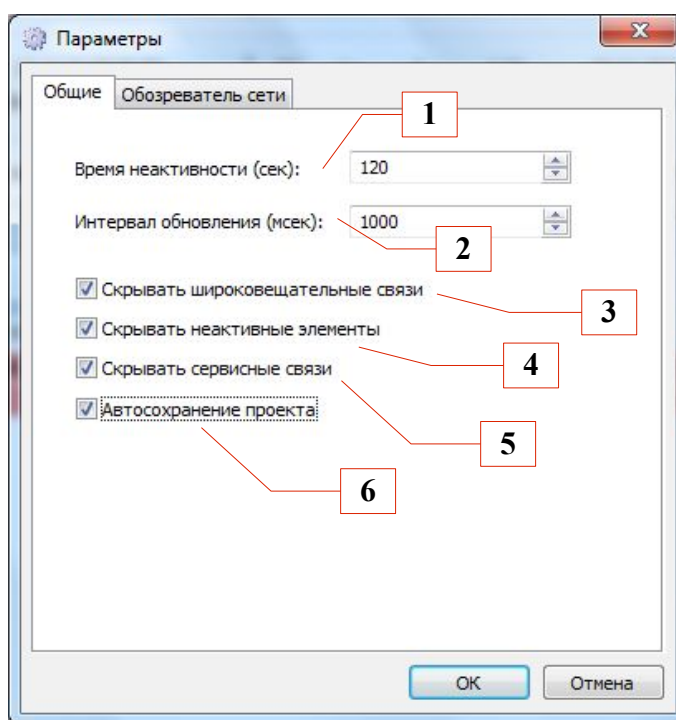


Рисунок 8- Окно настроек программы

1- Время неактивности (сек) — устанавливает временной интервал в течении которого объект должен передать пакет информации, в противном случае устройство будет признано неактивным и выделено в списке серым шрифтом.

2- Интервал обновления (мсек) — устанавливает интервал между циклами сканирования в секундах и, соответственно, обновлением всех списков во всех рабочих окнах программы.



Вычислительные мощности некоторых ПЭВМ могут быть недостаточны для обработки большого количества устройств и соединений при обновлении в несколько секунд. В этом случае рекомендуем увеличить интервал обновления.

При высокой производительности ПЭВМ (частота более 2ГГц для двух-ядерного процессора), рекомендуется интервал обновления 2-4 секунды, на ПЭВМ меньшей производительности: 10-15 секунд или более.

WiFi устройства, при работе в штатном режиме, посылают маяки опроса состояния с интервалом от нескольких раз в секунду до 1 раза в минуту. Таким образом, рекомендованный интервал неактивности, равный 60 секундам, обеспечит достоверное присвоение статуса активности обнаруженным устройствам и соединениям.

3- Скрывать широковещательные связи.

Точки доступа могут рассылать широковещательные (Broadcast) или

адресные (Multicast) сервисные пакеты. В этих случаях в числе соединений клиентов или точки доступа будут связи Broadcast, Multicast.

Что бы скрыть такие соединения в списке соединений необходимо поставить галочку в этом пункте.

По умолчанию широковещательные соединения скрываются.

4- Скрывать неактивные элементы.

Скрывает все элементы со статусом неактивный.

После ввода настроек, необходимо нажать «ОК». В результате, все изменения вступят в силу, а окно настроек закроется.

5- Скрывать сервисные связи.

В числе отображаемых клиентов точки доступа могут быть как ее «реальные» клиенты (устройства передающие трафик данных через эту точку доступа) так и «виртуальные» - те у которых включен режим активного поиска. Находясь в активном поиске клиент рассылает пакет с запросом состояния всем видимым ему устройствам (Probe request). Точка доступа получив такой запрос автоматически отвечает (Probe response) на него и клиент помещается в число ее клиентов, хотя больше может не разу с ней не контактировать и трафика через нее не пересылать.



Не стоит удалять таких «виртуальных» клиентов не убедившись, что они не представляют опасности, потому что таких «виртуальных» клиентов могут оказаться устройства с недекларированными возможностями находящиеся в режиме ожидания.

Чтобы скрыть все соединения в которых нет реальной передачи информации (трафика данных) используется этот пункт меню Настройки.

По умолчанию все сервисные соединения скрыты.

6- Автосохранение проекта.

Автоматически сохраняет каждые 5 минут: текущий проект, расположение рабочих окон.

5.2.2 Обозреватель сети

Позволяет выбрать активный сетевой интерфейс который будет использоваться программой для подключения к приемнику. Если на компьютере, на котором установлена программа есть несколько сетевых интерфейсов, например Ethernet и WiFi, то в этом пункте можно переопределить активный сетевой интерфейс, независимо от настроек ОС.

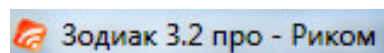
5.3 Создание нового проекта



После запуска программы автоматически загружается текущий проект,

или если запуск программы первый - загружается пустой проект.

Проектом называется совокупность данных об обнаруженных устройствах и соединениях WiFi и Bluetooth.

Название текущего проекта отображается в левом верхнем углу Рабочего пространства через дефис после номера версии программы (по умолчанию - «Новый проект»)



Создать новый Проект можно в любой момент работы программы нажатием кнопки  на панели инструментов или выбрать пункт главного Файл/Новый проект. После нажатия кнопки  появится информационное окно, представленное на рисунке 9, в котором необходимо подтвердить создание нового проекта.

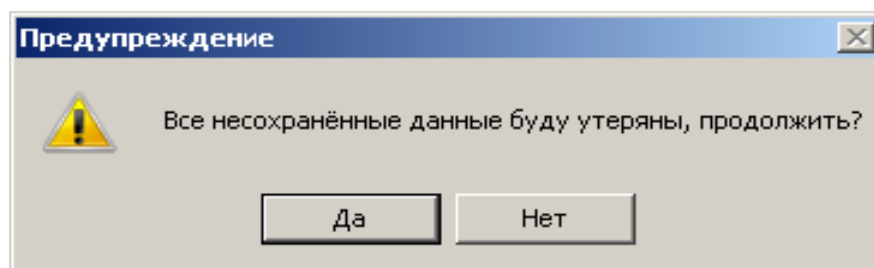


Рисунок 9 - Диалоговое окно подтверждения создания нового проекта





Для очистки текущего проекта также необходимо создать новый проект.



При создании нового проекта происходит удаление текущего Проекта без возможности его последующего восстановления.

5.4 Открытие проекта из внешнего файла

Сохраненный ранее проект может быть открыт из внешнего файла проектов. Файлы проектов имеют расширение «.zpr». Для загрузки проекта из внешнего файла необходимо нажать кнопку  на Панели инструментов или выбрать пункт меню Файл/Открыть проект. После нажатия кнопки  появится предупреждение о том, что все несохраненные данные будут потеряны, аналогичное как при создании нового проекта.

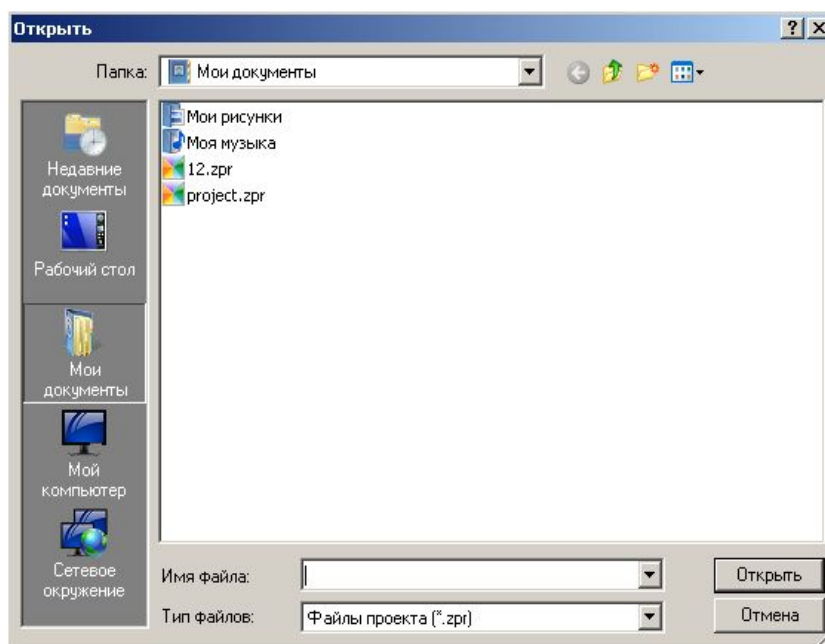



Рисунок 10 - Диалог открытия файла проекта

После нажатия кнопки «ОК» появится диалог открытия файла проекта, представленный на рисунке 10. В данном диалоге необходимо выбрать нужный файл проекта и нажать кнопку «Open». Нажатие кнопки «Cancel» приведет к возврату текущего проекта.



При открытии проекта происходит удаление текущего Проекта без возможности его последующего восстановления.

5.5 Сохранение проекта во внешний файл

Текущий проект может быть сохранен во внешний файл. Для этого необходимо нажать кнопку  на панели инструментов или выбрать в меню пункт Файл/Сохранить проект. В результате, откроется диалог сохранения проекта, представленный на рисунке 11. В поле «Имя файла» необходимо ввести название файла проекта и нажать «Save».

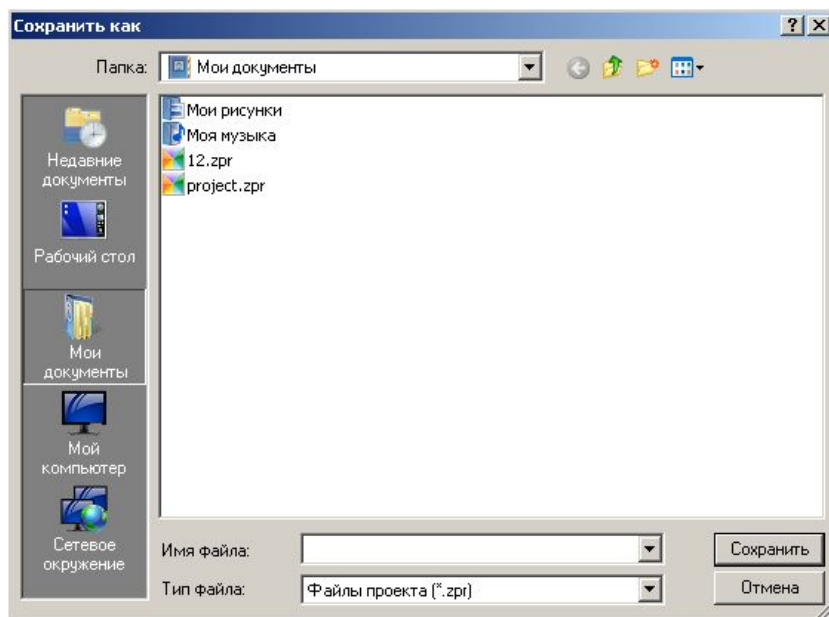


Рисунок 11 - Диалог сохранения проекта

По умолчанию все проекты оператора сохраняются в папке /Мои Документы с расширением «.zpr» .

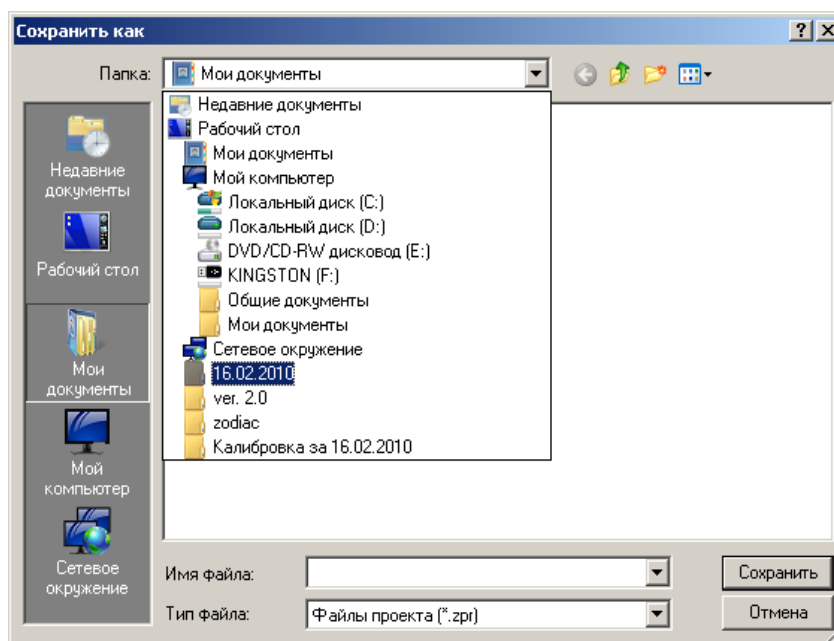


Рисунок 12- Изменение пути сохранения проекта

Для изменения пути воспользуйтесь адресным окном (рис. 12).





Если программа используется для анализа сетей нескольких объектов, то необходимо для каждого объекта создать свой

файл проекта и работать на каждом объекте со своим проектом.

5.6 Запуск и остановка режима сканирования

Перед запуском режима сканирования необходимо убедиться, что приемник подключен см **главу 3.1**. В противном случае кнопка начала сканирования будет недоступна.

Запуск и остановка сканирования производится по всем режимам одновременно кнопкой  на Панели инструментов или выбором пункта главного меню Действие/Сканирование.

Останавливается сканирование кнопкой .

В процессе сканирования происходит заполнение таблиц «Устройства WiFi», Устройства «Bluetooth» и «Соединения». Устройства и связи попадают в таблицу сразу в момент появления, а обновляются в таблице с интервалом обновления, заданным в поле «Обновление» окна настроек программной оболочки (рисунок 8).



В режиме сканирование вычислительные мощности ПЭВМ используются по максимуму возможностей. По этому не рекомендуется открывать окно настроек, при включенном режиме сканирования.



При переходе ПЭВМ в спящий или ждущие режимы на некоторых моделях ПЭВМ возможно блокирование работы адаптеров WiFi и Bluetooth операционной системой. Если после выхода из этих режимов не удастся запустить режим сканирования — следует перезагрузить ПЭВМ.

5.7 Выбор языка

Программа имеет мультязычный интерфейс: русский и английский. Язык программы выбирается автоматически в соответствии с текущим языком операционной системы.

6 Окна





6.1 Окно Устройства WiFi

Внешний вид окна «Устройства WiFi» для режима WiFi представлен на рисунке 13.

Имя	MAC адрес	Тип	Активность	Обнаружено	Время	Описание
Точки доступа						
Newsite	00:24:01:BC:7D:F9	bg	1	0.63	15.02.2010...	24.02.2...
Yota_newsite	0A:26:18:9F:C6:9C	bg	1	1.00	15.02.2010...	24.02.2...
Beeline_WiFi_WPA	00:19:E1:FF:BE:72	b	0	0.03	14.02.2010...	17.02.2...
Beeline_WiFi	00:19:E1:FF:BE:71	b	0	0.03	14.02.2010...	17.02.2...
Golden_WiFi	00:19:E1:FF:BE:70	b	0	0.02	14.02.2010...	17.02.2...
hide_net	00:22:B0:4F:BA:6A	bg	0	1.00	14.02.2010...	24.02.2...
00:18:B0:FE:16:E0	00:18:B0:FE:16:E0	b	0	0.01	14.02.2010...	17.02.2...
СНИТММТ	90:E6:BA:91:22:A5	b	1	1.00	14.02.2010...	24.02.2...
Beeline_WiFi	00:18:B0:FE:16:E1	b	0	0.01	14.02.2010...	17.02.2...
WL320gE	00:24:8C:69:B8:84	b	0	0.01	14.02.2010...	16.02.2...
Beeline_WiFi_WPA	00:18:B0:FE:16:E2	b	0	0.01	14.02.2010...	17.02.2...
Dor_stroy	00:26:5A:1C:F3:9C	b	0	1.00	16.02.2010...	16.02.2...
wireless	00:C0:02:D8:CA:68	b	0	0.01	16.02.2010...	16.02.2...
Клиенты						
miribr	00:40:96:53:26:D1	b	0	0.43	14.02.2010...	17.02.2...

Рисунок 13 - Внешний вид окна устройства WiFi

В окне отображается список всех обнаруженных WiFi устройств. Описание полей списка Устройств в режиме WiFi приведено в таблице 9.

Наименование	Обозначение	Описание
Выбор	<input checked="" type="checkbox"/>	Позволяет выбрать несколько объектов из списка. При установленной галочке <input checked="" type="checkbox"/> объект считается выбранным. Клик по шапке со значком Выбор позволяет выбрать все объекты списка или отменить такой выбор
Имя	нет	Отображает имя устройства. По умолчанию в данное поле заносится имя точки доступа (SSID) или MAC адрес устройства. Имена клиентов могут быть изменены оператором.
MAC адрес	нет	Отображает MAC адрес обнаруженного устройства.
Флаг		Отображает присвоенный пользователем флаг опасности для данного устройства: зеленый- легальное красный- опасное.
Тип устройства		Условное обозначение типа устройств
Тип интерфейса	Тип	Отображает типы интерфейса, которые поддерживаются обнаруженным устройством. Возможны варианты: a,b,g,n.*
Уровень		Отображает принимаемый уровень сигнала от устройства в графическом и цифровом виде в dBm. При изменении статуса устройства на неактивный сохраняет последний уровень сигнала принятый от этого устройства.
Рабочая частота	Частота (ГГц)	Отображает значение фактической рабочей частоты канала WiFi на которой работает устройство. В скобках отображается номер канала WiFi.
Связи		Отображает количество активных соединений, содержащих трафик данных, которые имеются у данного устройства на текущий момент (в этих соединениях устройство должно быть отправителем).
Передано	нет	Отображает объем переданного устройством суммарного трафика (данных и служебного трафика). Формат отображения объема данных: 100 = 100 байт; 1.1k = 1.1 кбайт; 1.1M = 1.1 Мбайт.
Принято	нет	Отображает объем полученного устройством суммарного трафика (данных и служебного трафика).

* Интерфейсы отображаются только если они поддерживаются комплексом.

Наименование	Обозначение	Описание
Активность	нет	Статистический параметр, показывающий насколько активно данное устройство обменивается данными с другими устройствами.
Обнаружено	нет	Отображает дату и время первого обнаружения устройства
Время	нет	Отображает дату и время последнего наблюдения устройства
Сессия	нет	Длительность последнего или текущего сеанса связи у устройства. Сеансом называется время нахождения устройства в статусе активного от момента появления или выхода из статуса неактивного.
Описание	нет	Текстовое поле с пользовательскими комментариями для устройства.

Таблица 9: Описание полей таблицы устройств

Если навести на строку списка указатель мыши, то в всплывающей подсказке для выбранного устройства будут отображены:

- производитель устройства;
- максимальный уровень сигнала от этого устройства;
- время обнаружения максимального уровня сигнала от этого устройства;
- текущий уровень сигнала от этого устройства;
- текущей уровень шума.



Для редактирования поля Имя необходимо дважды кликнуть по нему левой кнопкой мыши и изменить наименование устройства.



Используйте возможность для редактирования поля Имя для персонификации MAC адресов и устройств известных клиентов. На любом устройстве можно получить информацию о MAC адресе адаптера WiFi. После чего оператор может изменить поле Устройство назвав устройство именем владельца. Это позволит не только упростить анализ списка по критерию свой/чужой в дальнейшем, но и отслеживать активность легального клиента.



Для оценки активности устройства сравните значение поля Активность этого устройства и других устройств в списке.



Обычно неактивные устройства имеют 0 активных связей. Но если неактивному устройству передаются пакеты другим устройством то оно оставаясь неактивным может иметь количество активных связей отличное от 0.



Если устройство имеет активную связь и в окне соединений получателя типа Broadcast, это означает что на устройстве постоянно включен режим активного поиска. Как правило, это характерно для легальных устройств, поскольку такой режим увеличивает потребляемый устройством ток.

Обозначения типов устройств приведено в таблице 10. Установленный значок 🗎 рядом с именем точки доступа говорит о том, что данная точка доступа поддерживает только зашифрованные соединения.

Пустое значение поля Уровень означает что устройство либо находится в сети Ethernet к которой подключена точка доступа, либо находится вне зоны радиовидимости комплекса. Для того что бы скрыть такие устройства в списке Устройств есть правило «Вне зоны».

В поле Тип отображается тип обнаруженного устройства:







Обозн.	Описание
	Точка доступа
	Скрытая точка доступа
	Ретранслятор
	Обычный клиент
	Неизвестное устройство
	Клиент сконфигурированный на соединение клиент-клиент (AdHoc)

Таблица 10: Типы устройств

Если устройство находится в сети Ethernet то значение, которое отображается в поле Тип - может быть некорректным.



Если вместо имени точки доступа (SSID) в соответствующей графе указан MAC адрес это может означать следующее:
 - не удалось определить MAC адрес точки доступа т.к. от нее принят только один пакет.
 При приеме следующего пакета имя точки доступа будет автоматически обновлено и заменено на текущий SSID.

- точка доступа работает в режиме «ретранслятор». Тогда в поле «режим работы» будет отображен значок, соответствующий режиму ретранслятора;

- точка доступа имеет скрытый SSID и к ней еще не было подключений. Тогда в поле «режим работы» будет отображен значок, соответствующий режиму скрытой точки доступа. SSID точки будет отображен сразу после первого подключения к ней клиента.

6.2 Работа со списком в окне Устройства WiFi.

6.2.1 Выделение устройства в списке

Выделение устройства производится щелчком левой кнопкой мыши на требуемом устройстве. При выделении устройства в списке Устройства WiFi происходит автоматический поиск данного устройства в списке Связи WiFi и наоборот.

6.2.2 Группировка списка

Для списка в окне Устройства WiFi предусмотрено две группы: Клиенты и Точки доступа.

Для просмотра обнаруженных точек доступа и клиентов необходимо раскрыть соответствующую группу, кликнув на название группы*.

Для того что бы свернуть соответствующую группу необходимо еще раз кликнуть на название группы.

В ОС Windows XP группы отображаются всегда развернутыми.

После сворачивания, рядом с названием группы в скобках отображается количество новых устройств в этой группе. Если новых устройств нет, цифра в скобках не отображается.



Если размеры групп не позволяют исследовать их оперативно, то после проверки всех текущих устройств в группе, сверните ее и как только в группе появиться новое устройство в скобках рядом с названием группы обновиться счетчик новых устройств.

6.2.3 Сортировка списка

Пользователь имеет возможность произвести сортировку списка (в порядке возрастания/убывания значения одного из столбцов).


Для операционной системы Windows XP сортировка возможна только в несгруппированном списке. В Windows Vista и XP сортировка возможна и для

* Доступно только для ОС Windows Vista и 7.

сгруппированных списков.



Сгруппированные списки сортируются только по группам. Т.е. сортировка производится по общему правилу, но в каждой группе индивидуально.

Для сортировки необходимо кликнуть левой кнопкой мыши на заголовке списка на шапке с названием столбца. В результате, рядом с подписью столбца появится знак , означающий сортировку по возрастанию.

Повторное нажатие приведет к сортировке по убыванию. Сортировка таблицы устройств осуществляется по следующим правилам:

- 1 - Сортировка производится совместно для клиентов и точек доступа.
- 2 - Числовые поля сортируются по возрастанию/убыванию значений.
- 3 - Строковые поля сортируются в алфавитном порядке, при этом, первыми идут цифры, потом заглавные буквы латинского алфавита, затем строчные буквы латинского алфавита, далее заглавные буквы русского алфавита и, наконец, строчные буквы русского алфавита.
- 4 - Атрибуты опасности сортируются по уровню опасности.
- 5 - Поля даты и времени сортируются в хронологическом порядке.
- 6 - При сортировке поля Устройство меняются местами группы Клиенты и Точки доступа.



Если необходимо, чтобы новые устройства отображались вверху таблицы, нужно произвести сортировку по полю Время.

6.2.4 Изменение набора полей

Для изменения вида отображаемых полей необходимо кликнуть правой кнопкой мыши по шапке с наименованиями полей списка и в появившемся контекстном меню снять галочки с ненужных полей или поставить галочки рядом с названиями нужных полей (рис. 14).

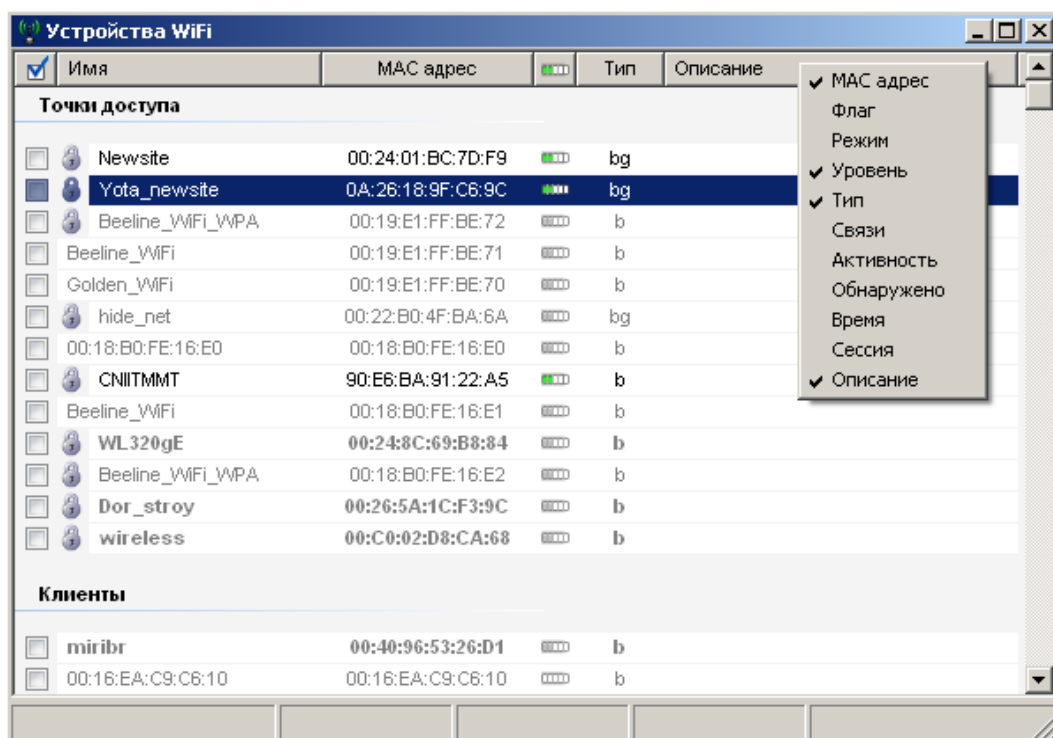


Рисунок 14- Изменение набора полей

Выбор пункта «Сбросить» в меню правой кнопки мыши приводит к восстановлению набора полей заданных в программе по умолчанию.




Настройка видимых полей производится по одному полю за одно отображение списка доступных полей.

6.2.5 Изменение положения и размера полей

Порядок следования полей списка может быть изменен по усмотрению оператора. Для этого необходимо нажать левую кнопку мыши на заголовке столбца и, не отпуская ее, перетащить столбец в нужную позицию (на место другого поля).

Нельзя изменить положение полей Выбор и Имя.

Ширина столбца также может быть изменена. Для этого необходимо привести указатель мыши на границу столбца, в результате, курсор изменит свой внешний вид на . После этого необходимо нажать левую кнопку мыши и, не отпуская ее, перетащить границу столбца вправо или влево, тем самым расширив или сузив его.



Установленные поля и их ширина сохраняются при сохранении проекта или при выходе из программы автоматически.

6.2.6 Редактирование имени клиента

При обнаружении клиента во время сканирования, он заносится в таблицу, при этом, по умолчанию, в качестве имени используется его MAC адрес. Поскольку на анализируемом объекте имеются штатные WiFi устройства, организующие работу беспроводных сетей, или встроенные в средства связи сотрудников, Пользователь имеет возможность заменить имя таких устройств в таблице самостоятельно на более удобные для пользователя, чем MAC адреса. Для этого в поле «Устройство» в выпадающем списке «Клиенты» необходимо произвести двойное нажатие левой кнопки на имени клиента. В результате, данное поле откроется для редактирования и в нем появится курсор. Пользователь должен ввести туда имя клиента, как это показано на рисунке 15, и нажать клавишу «Enter». Как правило, MAC адрес WiFi устройства указывается на обороте (этикетке) устройства или в инструкциях к нему.



Если поле Имя не редактировалось пользователем, то при работе правил этот клиент имеет статус «без имени».

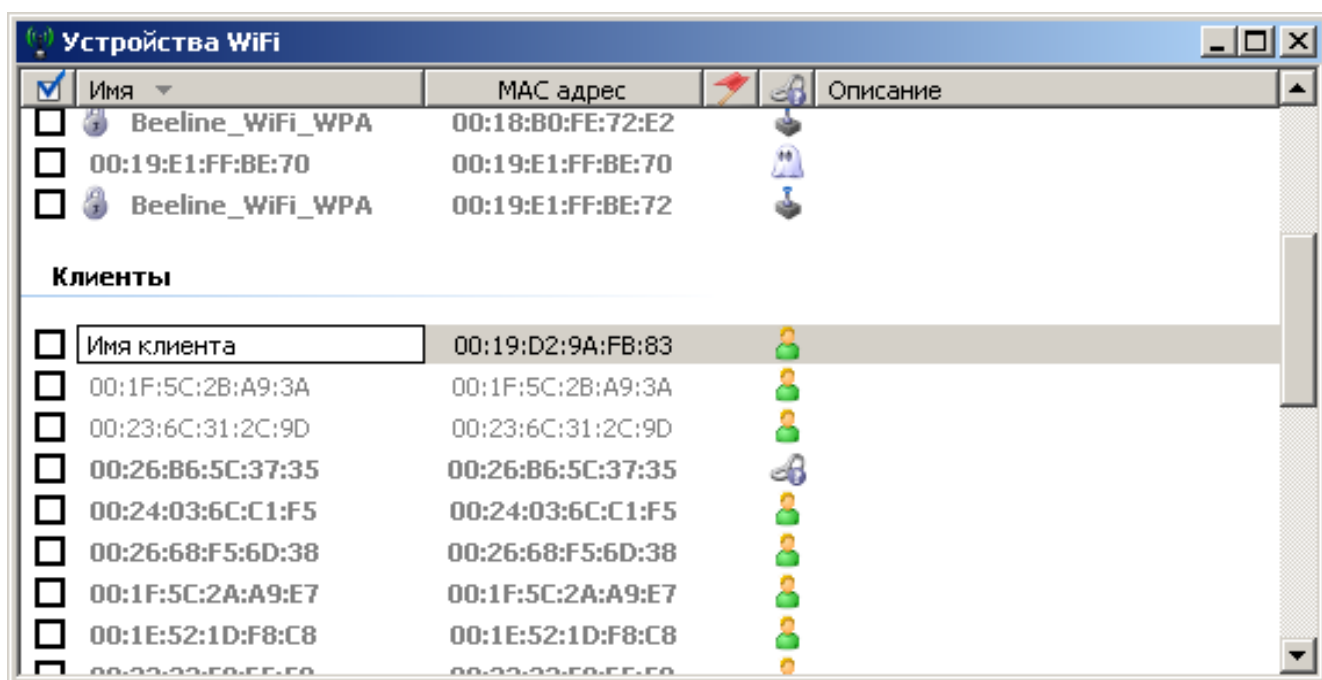


Рисунок 15 - Ввод имени клиента



Введенное имя клиента будет автоматически изменено в таблице «Соединения WiFi», а также в других окнах («Граф» и «Монитор»). Используя удобные имена, вместо MAC адресов, оператор облегчает себе анализ трафика данных и таблицы соединений.



Имя клиента, работающего в режиме клиент-клиент изменить нельзя.

6.2.7 Навигация в окне Устройства WiFi

Навигация в окне устройства осуществляется с помощью мыши и через контекстное меню правой кнопки мыши.

Команды контекстного меню приведены в таблице 11.

Наименование	Описание
Пометить известным	Атрибут «неизвестные» будет автоматически снят со все объектов выбранных в поле Выбор. Соответственно будет снято выделение жирным шрифтом со строк.
Группировка	Включает/выключает режим группировки
Флаг	
- Неизвестное	Снимает с устройства флаги Легальное и Опасное
-Легальное	Ставит на устройство флаг Легальное
-Опасное	Ставит на устройство флаг Опасное
Граф	Открывает окно Графа для выбранного объекта списка
Скрыть	Скрывает устройство в списке. При скрывании устройства слева от пункта меню появляется галочка. При повтором выборе пункта на скрытом устройстве — оно изменяет статус на не скрытое и галочка пропадает
Удалить устройство	Удаляет устройство из списка

Таблица 11: Контекстное меню правой кнопки мыши




Команда «Удалить устройство» удаляет его из списка без возможности восстановления. Если вы не уверены в необходимости такого удаления лучше воспользоваться командой «Скрыть устройство».


6.2.8 Изменение флага устройства

Пользователь каждому устройству может присвоить флаг:

1 - Неизвестное устройство. Присваивается по умолчанию

обнаруженным устройствам. Поле «Атрибут» таблицы устройств пустое.

2 - Опасное устройство. В поле «Атрибут» данного устройства появляется значок .

3 - Легальное устройство. В поле «Атрибут» данного устройства появляется значок .





Для изменения атрибута выбранного устройства, необходимо в контекстном меню выбрать пункт «Флаг» и выбрать атрибут из подменю.

6.2.9 Скрытие устройств в списке

После принятия решения о легальности устройства, Пользователь имеет возможность скрыть его для уменьшения количества отображаемых строк списка. Для этого необходимо выбрать в контекстном меню пункт «Скрыть устройство». При этом, устройство не будет отображаться в списке, хотя оно останется в данном проекте.



Если скрывается устройство, которое является Отправителем для какой либо связи, скрывается и вся группа связи в окне Соединения. Если скрывается устройство, которое является Получателем в какой либо группе связей, то в окне Соединения скрывается только связь с этим устройством.

Для просмотра скрытых устройств необходимо в инструментальной панели главного окна нажать кнопку . В результате, все скрытые устройства будут показаны и кнопка изменит вид на . При этом, имя скрытых устройств будет отображаться курсивным шрифтом. После отжатия кнопки  все скрытые соединения будут скрыты и кнопка изменит вид на .



Следует помнить что устройства могут скрываться вручную оператором, в настройках программы и с помощью правил.



Курсивным шрифтом в списке отображаются только устройства скрытые вручную и правилами. Устройства скрытые в настройках курсивом не отображаются.

6.2.10 Удаление устройства из списка

Любое устройство может быть удалено из списка без возможности восстановления. Для этого необходимо выбрать в контекстном меню пункт «Удалить устройство».



Если удаленное устройство будет обнаружено при следующем сканировании, то оно снова появится в таблице как новое устройство.

6.3 Окно Связи WiFi

Внешний вид окна «Связи WiFi» представлен на рисунке 16.

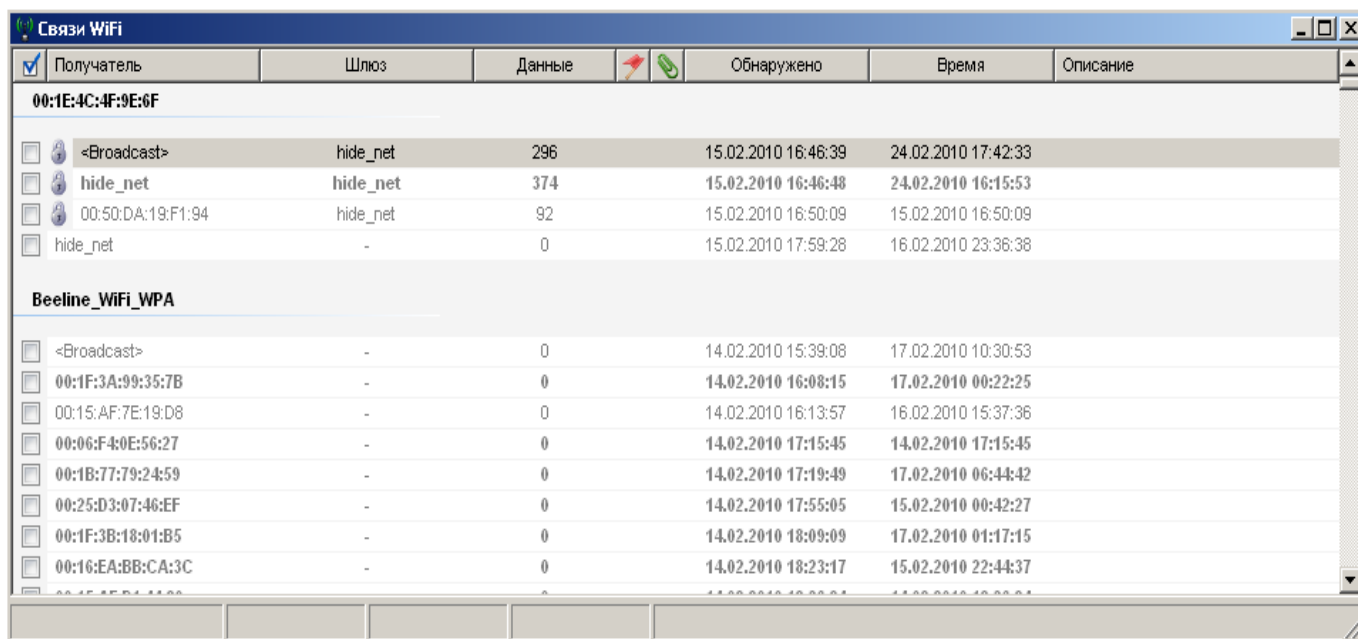


Рисунок 16 - Внешний вид окна Связи WiFi

В окне отображается список всех обнаруженных соединений устройств WiFi.



Редактировать имена устройств в окне Связи WiFi нельзя. Для редактирования следует воспользоваться окном Устройства.

Описание полей окна Связи WiFi приведено в таблице 12.

Наименование	Обозначение	Описание
Выбор	<input checked="" type="checkbox"/>	Позволяет выбрать несколько объектов из списка. При установленной галочке <input checked="" type="checkbox"/> объект считается выбранным. Клик по шапке со значком Выбор позволяет выбрать все объекты списка или отменить такой выбор.
Отправитель	нет	Отображает поле Имя отправителя
Получатель	нет	Отображает поле Имя получателя
Шлюз	нет	Отображает имя устройства (как правило точки доступа), через которое Получатель связывается с Отправителем или внешней сетью.


Наименование	Обозначение	Описание
Флаг		Отображает присвоенный пользователем флаг опасности для данной связи: зеленый- легальное красный- опасное.
История		Отображает флаг наличия записанной истории соединения
Доля	%	Отображает долю пакетов (в процентах), относящихся к данному соединению, относительно всех соединений данного устройства
Обнаружено	нет	Отображает дату и время первого обнаружения связи
Время	нет	Отображает дату и время последнего наблюдения связи
Сессия	нет	Отображает длительность текущего сеанса связи
Данные	нет	Отображает объем переданных данных во время связи. Формат отображения объема данных: 100- 100 байт 1.1к- 1.1 кбайт 1.1М- 1.1 МБайт
Служебное	нет	Отображает объем переданных служебных данных во время связи. Формат поля аналогичен полю Данные
Описание	нет	Поле для ввода пользовательских комментариев

Таблица 12: Описание полей таблицы соединений



Значения трафика данных и служебного трафика являются оценочными и могут отличаться от реальных значений.

6.4 Работа со списком в окне Связи WiFi

6.4.1 Выделение соединений в списке

Выделение соединений производится нажатием левой кнопки мыши на требуемом соединении. При выделении устройства в списке Устройства WiFi происходит автоматический поиск данного устройства в списке Связи WiFi и наоборот.



В процессе сканирования происходит постоянная перестройка списка. Но если выделить соединение, то оно не будет перемещаться по списку при добавлении новых групп соединений.

6.4.2 Группировка списка

Список может быть сгруппирован по следующим полям:

- поле Отправитель
- поле Получатель
- Поле Шлюз

Группировка осуществляется из меню правой кнопки мыши, пункт Группировка.

В зависимости от типа группировки первые два отображаемых поля списка могут изменяться:

- при группировке по полю Отправитель- первые два поля всегда Получатель и Шлюз;
- при группировке по полю Получатель- первые два поля всегда Отправитель и Шлюз;
- при группировке по полю Шлюз- первые два поля всегда Отправитель и Получатель.

В названии группы всегда стоит поле по которому группируется список- при раскрытии групп, будут отображаться имена всех подчиненных ему устройств.

Понятие отправителя и получателя — ключевые понятия в интерфейсе программы. В любой связи в WiFi есть ведущее устройство и ведомое устройство. Обычно ведущим устройством в связи является точка доступа, одна при других вариантах соединения, когда точки доступа нет, например клиент-клиент, возможны варианты. Отправителем в программе называется ведущее устройство. Устройство отправитель может и принимать информацию от получателя, но в их связи оно ведущее. Точно так же получатель может отправлять информацию оставаясь ведомым. Важно понимать что атрибут Отправитель и Получатель относятся скорее не к фактическому статусу устройства, а к его старшинству в связи.

Для сворачивания/раскрытия* соответствующей группы необходимо кликнуть на ее название.



По умолчанию все группы в окне Устройства свернуты. Не следует открывать слишком много групп, т.к. это существенно затрудняет работу со списком.

После сворачивания*, рядом с названием группы в скобках отображается количество новых соединений в этой группе. Если новых соединений нет, цифра в скобках не отображается.

6.4.3 Сортировка списка

Аналогично списку Устройства WiFi ([глава 6.2.3](#)).

* Доступно только в в ОС Windows Vista и 7.

6.4.4 Изменение набора полей

Аналогично списку Устройства WiFi (глава 6.2.4).

6.4.5 Изменение положения и размера полей списка

Аналогично списку Устройства WiFi (глава 6.2.5).

6.4.6 Навигация в списке

Для выбора связи в окне Соединений необходимо раскрыть группу и выбрать с помощью мыши получателя информации. После этого можно вызвать контекстное меню правой кнопки мыши. Контекстное меню при клике по названию группы открывается в сокращенном виде. Описание пунктов контекстного меню представлено в таблице 13.

Наименование	Описание
Свернуть / Развернуть	Сворачивает или разворачивает все группы в списке*
Пометить известным	Атрибут «неизвестные» будет автоматически снят со все объектов выбранных в поле Выбор. Соответственно будет снято выделение жирным шрифтом со строк.
Группировка	Включает/выключает режим группировки
- Без группировки	Отключает группировку
- {Отправитель}	Группирует по полю Отправитель
- {Получатель}	Группирует по полю Получатель
- {Шлюз}	Группирует по полю Шлюз
Флаг	
- Неизвестное	Снимает с устройства флаги Легальное и Опасное
-Легальное	Ставит на устройство флаг Легальное
-Опасное	Ставит на устройство флаг Опасное
Граф	Открывает окно Графа для выбранного Отправителя
Монитор	Открывает окно Монитор для выбранного Отправителя
Запись	Начинает/останавливает запись истории трафика для выбранного соединения
Удалить историю	Удаляет историю данного соединения
Скрыть	Скрывает устройство в списке. При скрытии устройства слева от пункту меню появляется галочка. При повтором выборе пункта на скрытом устройстве — оно изменяет статус на не скрытое и галочка пропадает

* Доступно только в ОС Windows Vista или 7.


Наименование	Описание
Удалить	Удаляет выбранное устройство из списков устройств и связей.


Таблица 13: Контекстное меню окна Соединений

6.4.7 Изменение флага соединения

Пользователь каждому соединению может присвоить флаг:

1 - Неизвестное соединение. Присваивается по умолчанию обнаруженным соединениям. Поле «Атрибут» пустое.

2 - Опасное устройство. В поле «Атрибут» данного устройства появляется значок .

3 - Легальное устройство. В поле «Атрибут» данного устройства появляется значок .

Для изменения флага выбранного соединения необходимо в контекстном меню выбрать пункт «Уровень опасности» и выбрать атрибут из подменю.

6.4.8 Скрытие соединений в списке

Аналогично списку Устройства WiFi ([глава 6.2.9](#))


6.4.9 Удаление соединения из списка

Любое соединение может быть удалено из списка без возможности восстановления. Для этого необходимо выбрать в контекстном меню пункт «Удалить соединение».




Если удаленное соединение будет обнаружено при следующем сканировании, то оно снова появится в таблице как новое соединение.


6.4.10 Запись истории соединения

Для выбранного соединения оператор может записать историю трафика для последующего анализа. Записывается текущий объем данных и служебных пакетов. Для записи необходимо в контекстном меню правой кнопки мыши выбрать пункт «Запись». Слева от пункта «Запись» в контекстном меню появится галочка. В поле «История» появиться значок .



Если поле «История» было скрыто оно автоматически появиться среди полей списка.

Для остановки записи необходимо повторно выбрать пункт контекстного меню «Запись». При этом галочка слева пропадет а иконка в поле «История» станет .

Для просмотра истории необходимо дважды нажать левую кнопку мыши на иконке  в поле «История», в результате, откроется окно «История» с историей данного соединения. Внешний вид окна воспроизведения истории аналогичен окну «Монитор» , которое будет рассмотрено в **главе 8**.



Не открывайте слишком много записей Истории, т.к. это может сказаться на производительности программы.



При выходе из оболочки программы, запись истории по всем соединениям останавливается автоматически.

6.5 Окно Устройства Bluetooth*

Внешний вид окна «Устройства Bluetooth» представлен на рисунке 17.

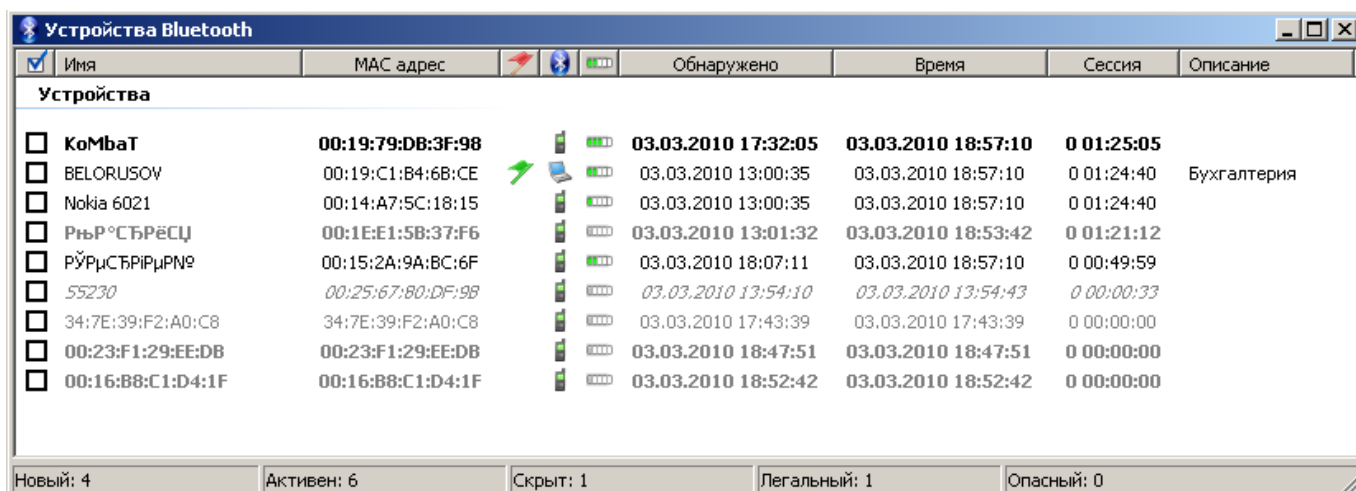


Рисунок 17: Внешний вид окна Устройства Bluetooth

Дерево окна Устройства Bluetooth имеет только группу Устройства. Раскрытие и сворачивание этой группы производится аналогично окну Устройства WiFi.

Описание полей списка Устройства Bluetooth приведено в таблице 14.

* Для работы комплекса в режиме обнаружения устройств, использующих беспроводной стандарт передачи данных Bluetooth, требуется адаптер BT-11.




Наименование	Обозначение	Описание
Выбор	<input checked="" type="checkbox"/>	Позволяет выбрать несколько объектов из списка. При установленной галочке <input checked="" type="checkbox"/> объект считается выбранным. Клик по шапке со значком Выбор позволяет выбрать все объекты списка или отменить такой выбор
Имя	нет	Отображает имя устройства заданное на самом устройстве владельцем. Поле не редактируется оператором.
MAC адрес	нет	Отображает MAC адрес обнаруженного устройства
Флаг		Отображает присвоенный пользователем флаг опасности для данного устройства: зеленый- легальное красный- опасное.
Тип устройства		Условное обозначение типа устройства
Связи		Отображает количество активных соединений имеющихся у данного устройства на текущий момент
Активность	нет	Статистический параметр, показывающий насколько активно данное устройство обменивается данными с другими устройствами.
Обнаружено	нет	Отображает дату и время первого обнаружения устройства
Время	нет	Отображает дату и время последнего наблюдения устройства
Описание	нет	Текстовое поле с пользовательскими комментариями для данного объекта.

Таблица 14: Описание полей таблицы устройств

Обозначения типов устройств с интерфейсом Bluetooth приведено в таблице 15.






Обозначение	Описание
	Мобильный телефон
	Беспроводная гарнитура
	КПК
	Ноутбук
	Рабочая станция
	Неизвестное устройство

Таблица 15: Типы устройств

Устройства Bluetooth в состоянии поиска пары отображаются только если ранее они были в активном состоянии.

6.6 Работа со списком в окне Устройства Bluetooth

6.6.1 Сортировка списка

Аналогично списку Устройств WiFi (**глава 6.2.3**)

6.6.2 Изменение набора полей

Аналогично списку Устройств WiFi (**глава 6.2.4**)

6.6.3 Изменение положения и размера полей

Аналогично списку Устройств WiFi (**глава 6.2.5**)

6.6.4 Навигация в списке

Аналогично списку Устройств WiFi (**глава 6.2.7**)

6.6.5 Изменение флага устройства

Аналогично списку Устройств WiFi (**глава 6.2.8**)

6.6.6 Скрытие устройства в списке

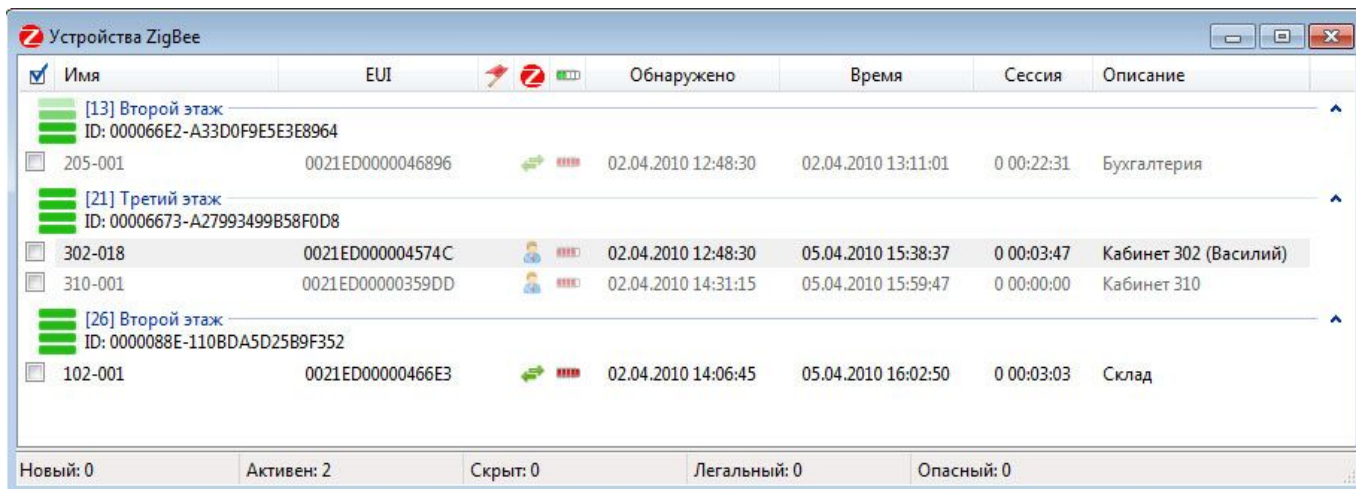
Аналогично списку Устройств WiFi (**глава 6.2.9**)

6.6.7 Удаление устройства из списка

Аналогично списку Устройств WiFi (**глава 6.2.10**)

6.7 Окно Устройства ZigBee*

Внешний вид окна «Устройства ZigBee» представлен на рисунке 18.



Имя	EUI	Статус	Обнаружено	Время	Сессия	Описание
[13] Второй этаж ID: 000066E2-A33D0F9E5E3E8964						
205-001	0021ED0000046896		02.04.2010 12:48:30	02.04.2010 13:11:01	0 00:22:31	Бухгалтерия
[21] Третий этаж ID: 00006673-A27993499B58F0D8						
302-018	0021ED000004574C		02.04.2010 12:48:30	05.04.2010 15:38:37	0 00:03:47	Кабинет 302 (Василий)
310-001	0021ED00000359DD		02.04.2010 14:31:15	05.04.2010 15:59:47	0 00:00:00	Кабинет 310
[26] Второй этаж ID: 0000088E-110BDA5D25B9F352						
102-001	0021ED00000466E3		02.04.2010 14:06:45	05.04.2010 16:02:50	0 00:03:03	Склад

Новый: 0 Активен: 2 Скрыт: 0 Легальный: 0 Опасный: 0

Рисунок 18: Внешний вид окна Устройства ZigBee

Дерево окна Устройства ZigBee имеет только группу Устройства. Раскрытие и сворачивание этой группы производится аналогично окну Устройства WiFi.

Описание полей списка Устройства ZigBee приведено в таблице 16.

* Для работы комплекса в режиме обнаружения устройств, использующих беспроводной стандарт передачи данных ZigBee, требуется адаптер ZB-11.




Наименование	Обозначение	Описание
Выбор	<input checked="" type="checkbox"/>	Позволяет выбрать несколько объектов из списка. При установленной галочке <input checked="" type="checkbox"/> объект считается выбранным. Клик по шапке со значком Выбор позволяет выбрать все объекты списка или отменить такой выбор
Уровень		Интегральный уровень сигнала в канале сети
Частота (ГГц)	нет	Отображается номинал рабочей частоты канала ZigBee на котором работает устройство.
Имя	нет	Отображает имя устройства. По умолчанию в данное поле заносится EUI обнаруженного устройства.
EUI	нет	Отображает сетевой адрес (EUI) обнаруженного устройства.
Флаг		Отображает присвоенный пользователем флаг опасности для данного устройства: зеленый- легальное красный- опасное.
Тип устройства		Условное обозначение типа устройств
Уровень		Отображает принимаемый уровень сигнала от устройства в графическом и цифровом виде в dBm. При изменении статуса устройства на неактивный сохраняет последний уровень сигнала принятый от этого устройства.
Обнаружено	нет	Отображает дату и время первого обнаружения устройства
Время	нет	Отображает дату и время последнего наблюдения устройства
Сессия	нет	Длительность последнего или текущего сеанса связи у устройства. Сеансом называется время нахождения устройства в статусе активного от момента появления или выхода из статуса неактивного.
Описание	нет	Текстовое поле с пользовательскими комментариями для устройства.

Таблица 16: Описание полей таблицы устройств

Обозначения типов устройств с интерфейсом ZigBee приведено в таблице 17.




Обозначение	Описание
	Конечное устройство
	Координатор
	Маршрутизатор

Таблица 17: Типы устройств

6.8 Работа со списком в окне Устройства ZigBee

6.8.1 Сортировка списка

Аналогично списку Устройств WiFi (**глава 6.2.3**)

6.8.2 Изменение набора полей

Аналогично списку Устройств WiFi (**глава 6.2.4**)

6.8.3 Изменение положения и размера полей

Аналогично списку Устройств WiFi (**глава 6.2.5**)

6.8.4 Навигация в списке

Аналогично списку Устройств WiFi (**глава 6.2.7**) за одним исключением: команды «Флаг» в контекстном меню окна Устройства ZigBee нет.

6.8.5 Изменение флага устройства

Аналогично списку Устройств WiFi (**глава 6.2.8**)

6.8.6 Скрытие устройства в списке

Аналогично списку Устройств WiFi (**глава 6.2.9**)

6.8.7 Удаление устройства из списка

Аналогично списку Устройств WiFi (**глава 6.2.10**)

7 Окно Граф

7.1 Назначение режима графа

Режим графа предназначен для графической визуализации связей выбранного устройства.



Граф строится только для объектов WiFi.

На графе отображаются:

- 1 - Все связи данного устройства с другими устройствами напрямую и через шлюз (через точку доступа).
- 2 - Все широковещательные запросы данного устройства.
- 3 - Все перекрестные связи (кросс-связи) устройств, то есть связи устройств входящих в сеть анализируемого устройства между собой напрямую или через шлюз.

Количество окон Граф не ограничено.

7.2 Переход в режим графа

Переход в режим Граф возможен двумя способами:

- 1 - Запуск окна «Граф» из главного меню программы Инструменты-Граф. При этом откроется граф выбранного устройства. Устройство для построения графа можно выбирать и в окне Устройства WiFi и Связи WiFi.

- 2 - Запуск из контекстного меню правой кнопки мыши пункт Граф.

7.3 Внешний вид и описание окна графа

При запуске окна «Граф» откроется окно представленное на рисунке 19.

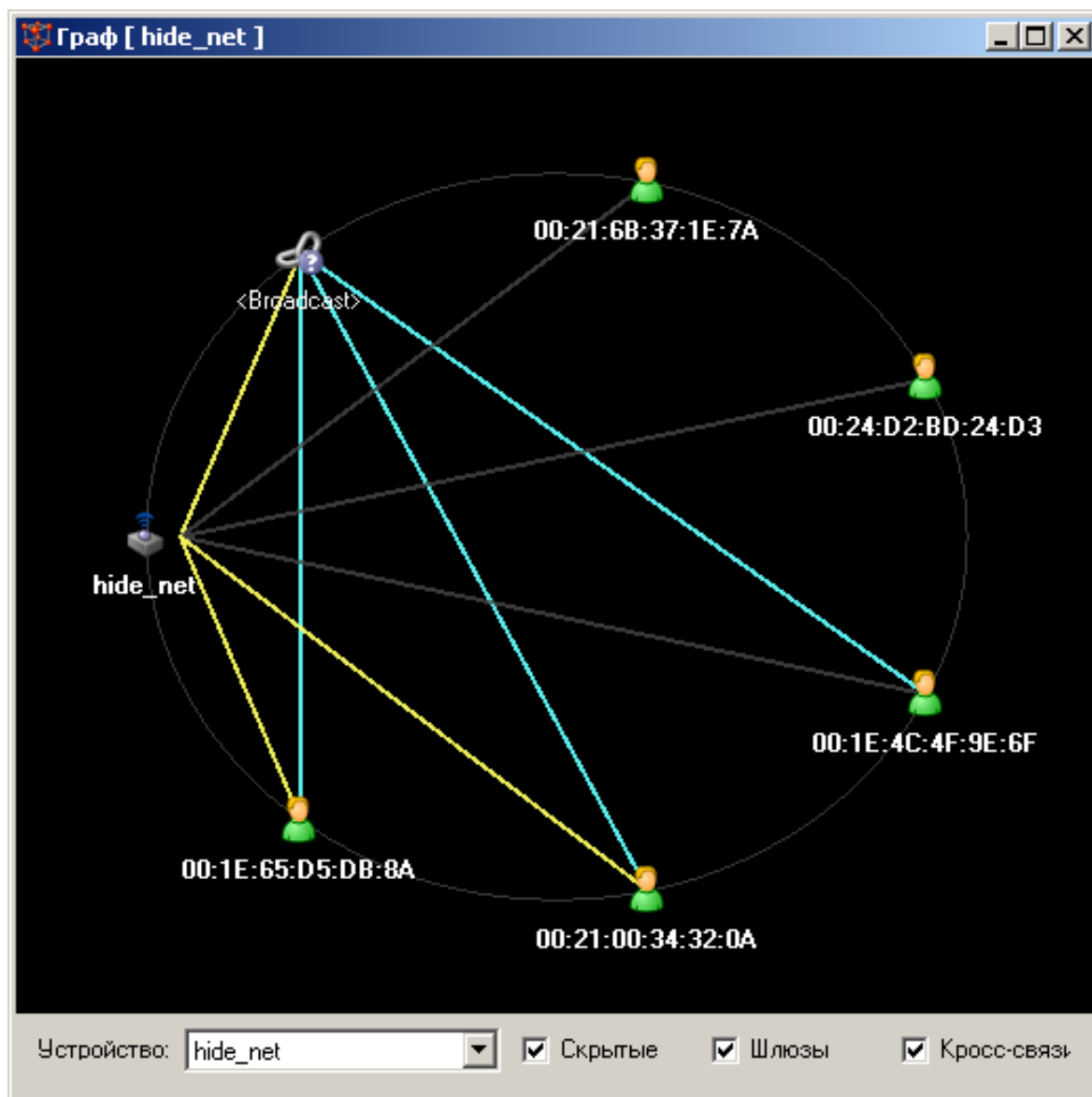


Рисунок 19 - Внешний вид окна Граф

В центральной области окна: графическое представление сети выбранного устройства. В нижней части, в выпадающем списке, можно выбрать имя устройства, сеть которого требуется отобразить. По умолчанию, используется имя устройства, которое было выбрано при переходе в режим графа.

Выбранное устройство всегда расположено слева по центру. Сеть данного устройства расположена по окружности правее. Графически отображаются типы устройств, с которыми связано данное устройство, имена устройств подписываются снизу.

Активные связи отображаются желтым цветом.

Серым цветом отображаются неактивные связи.


Жирной линией отображаются новые связи, не жирной- не новые.

Установленная внизу окна галочка «Шлюзы» отображает точки доступа (если таковые имеются) через которые связаны устройства.

Установленная внизу окна галочка «Кросс-связи» отображает все перекрестные связи устройств. Кросс-связи отображаются голубыми линиями.

Установленная внизу окна галочка «Скрытые» позволяет отобразить скрытые связи устройств серым цветом. Синими цветом отображаются связи скрытые вручную.



При включенном режиме «Показатель скрытые»  на графе будут отображаться все связи независимо от установок в окне Графа.

Имена опасных устройств выделяются красным, а связи на графе отображаются красной линией.

В процессе сканирования граф отображает все текущие связи. При изменении дерева соединений, граф автоматически перестраивается. При обнаружении нового устройства, подпись под ним отображается жирным шрифтом.



С помощью мыши можно изменить размер окна и его местоположение. Пovedите указатель мыши к границе окна и удерживая нажатой левую кнопку мыши перетащите границу в нужное положение. Наведите указатель мыши на шапку окна и удерживая нажатой левую кнопку мыши перетащите окно в любое место экрана.

8 Окно Монитор

8.1 Назначение режима монитора

Режим монитора предназначен для визуального контроля распределения трафика данных и служебного трафика между двумя устройствами в режиме соединения.



Режим монитор доступен только из окна Связи WiFi.

Анализ возможен на нескольких временных интервалах от 10 минут до 24 часов.

Для динамического отображения объема передаваемого трафика в окне монитор должно быть запущено сканирование. Количество окон Монитор не ограничено.



При включенном режиме Монитор приемник перестает сканировать частотные каналы WiFi и принимает сигнал только на одном канале, соответствующем выбранному в режиме Монитор устройству. Соответственно, при включенном режиме Монитор обновление списка устройств происходит частично. Для полноценно сканирования необходимо отключить режим Монитор. Если открыто несколько окно Монитор, то приемник фиксируется на частоте, которая соответствует активному окну. Если выбрать активным окно Устройств или Связей WiFi нормальное сканирование восстановиться, но в окне(ах) монитор будет неполноценная информация.

8.2 Переход в режим монитора

Переход в режим граф возможен двумя способами:

1 - Запуск окна «Монитор» из главного меню программы Инструменты-Монитор. При этом, откроется окно монитора устройства, выбранного в окне Соединения.

2 - Запуск из контекстного меню правой кнопки мыши, пункт Монитор, для устройств в списке Связи WiFi.

8.3 Внешний вид и описание окна монитора

При запуске окна «Монитор» откроется окно представленное на рисунке

20.

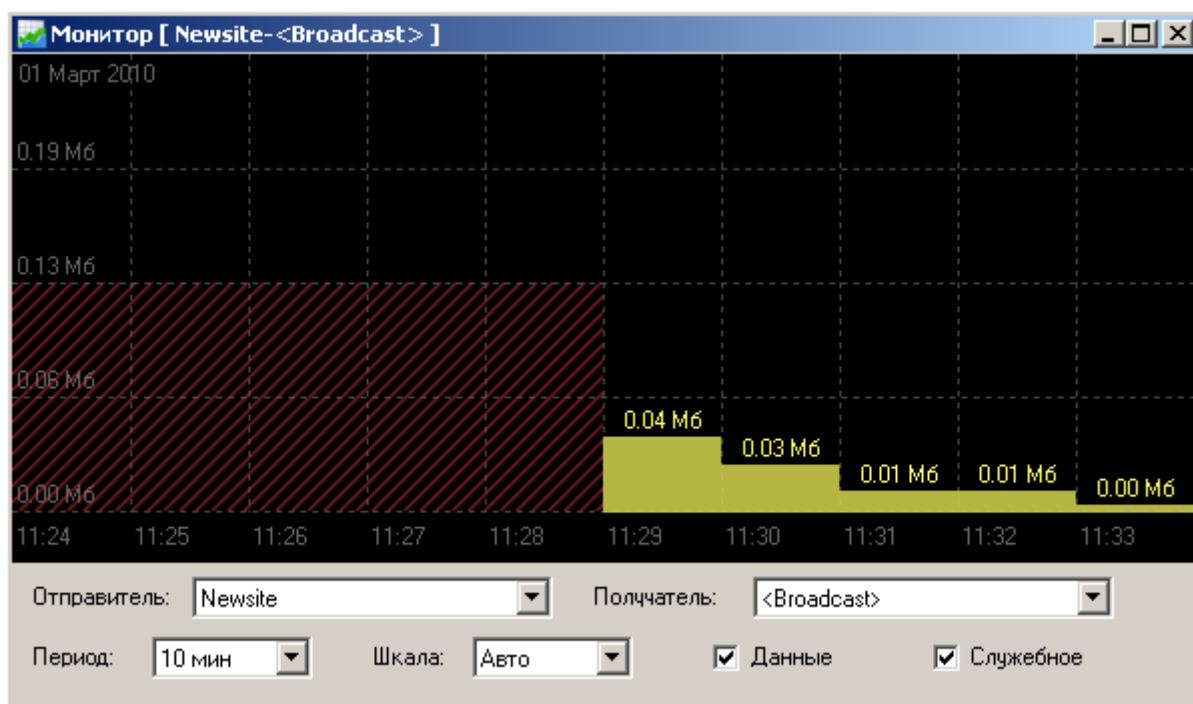


Рисунок 20 - Окно Монитор

В центральной области окна гистограмма служебного трафика и трафика данных. Служебный трафик отображается желтым цветом, трафик данных — зеленым.

В выпадающих списках «Отправитель» и «Получатель» нужно выбрать устройства, соединения которых требуется анализировать. При запуске окна «Монитор» из контекстного меню таблицы соединений в данных полях автоматически выбираются устройства, выбранные в таблице соединений. Выпадающий список «Период» устанавливает время анализа от 10 минут до 24 часов.

Выпадающий список «Шкала» позволяет установить верхнюю границу шкалы трафика. По умолчанию, верхняя граница выбирается автоматически.

Галочками «Данные» и «Службные» отмечаются какой трафик анализируется.

При просмотре данных в окне «Монитор», вращая колесико мыши вверх, можно прокрутить данные за пределы участка анализа. Вращение колесика вниз вернет текущее временное положение данных.



Воспользуйтесь колесом скроллинга мыши для перемещения картинки в окне монитор влево-вправо.



С помощью мыши можно изменить размер окна и его местоположение. Поведите указатель мыши к границе окна и

удерживая нажатой левую кнопку мыши перетащите границу в нужное положение. Наведите указатель мыши на шапку окна и удерживая нажатой левую кнопку мыши перетащите окно в любое место экрана.

9 Правила

9.1 Назначение правил

Правила — инструмент автоматизированного анализа списка и отбора сигналов по разведпризнакам, позволяющий выделить устройства и соединения, представляющие потенциальную опасность, а также штатные устройства.

В правилах реализован механизм задания критерия отнесения устройства и соединения к легальным и опасным на основе комбинаций разведпризнаков. Например, потенциально-опасной можно считать точку доступа со скрытым именем и зашифрованным каналом данных, которая имеет низкую активность, но периодически передает некоторое количество данных.



Комплекс поставляется с набором стандартных правил. Для экспорта нового списка правил необходимо скопировать следующий файл: `.../zodiac/rules.dat`. Для импорта списка правил необходимо заменить этот же файл. Правила можно экспортировать/импортировать только полным списком.




Не рекомендуется создавать новые или изменять правила поставляемые с программой неопытным пользователям. Советуем воспользоваться имеющимся набором правил.

В дистрибутив программы включены следующие правила:

- «Близкое устройство» правило предназначено для выделения красным цветом строчек с устройствами WiFi у которых уровень больше -50dBm , это может означать, что устройство находится в ближней зоне комплекса.
- «Вне зоны» правило предназначено для скрытия в списке WiFi устройств уровень которых не определен, это может означать, что устройство находится вне зоны радиовидимости комплекса и определяется комплексом по вторичной информации от точек доступа, а не напрямую по собственным пакетам устройства.
- «Близкое устройство BT» правило предназначено для выделения красным цветом строчек с устройствами Bluetooth у которых уровень больше -70dBm , это может означать, что устройство находится в ближней зоне комплекса.

9.2 Окно Правила

Правила создаются в окне настроек , которое вызывается с помощью кнопки  на панели инструментов или из главного меню Инструменты-Правила. В результате откроется окно, представленное на рисунке 21.

Окно настроек состоит из следующих областей:

1- область структуры правил


2- папки с правилами

3- правила

4- значок типа правил.

5- поле активности правила. При выбранном поле правило применяется для обработки списка немедленно при нажатии Ок или Применить.

6- область ввода названия правила

7- поле ввода типа правила; правила в программе могут быть трех типов: Устройства WiFi , Связи WiFi , Устройства Bluetooth 

8- область ввода условия правила

9- область ввода действия правила.

10- кнопка Ок сохраняет изменения в правилах и закрывает окно правил.

11- Кнопка отменить - отменяет все изменения сделанные при последнем открытии окна настройки правил и закрывает окно настроек.

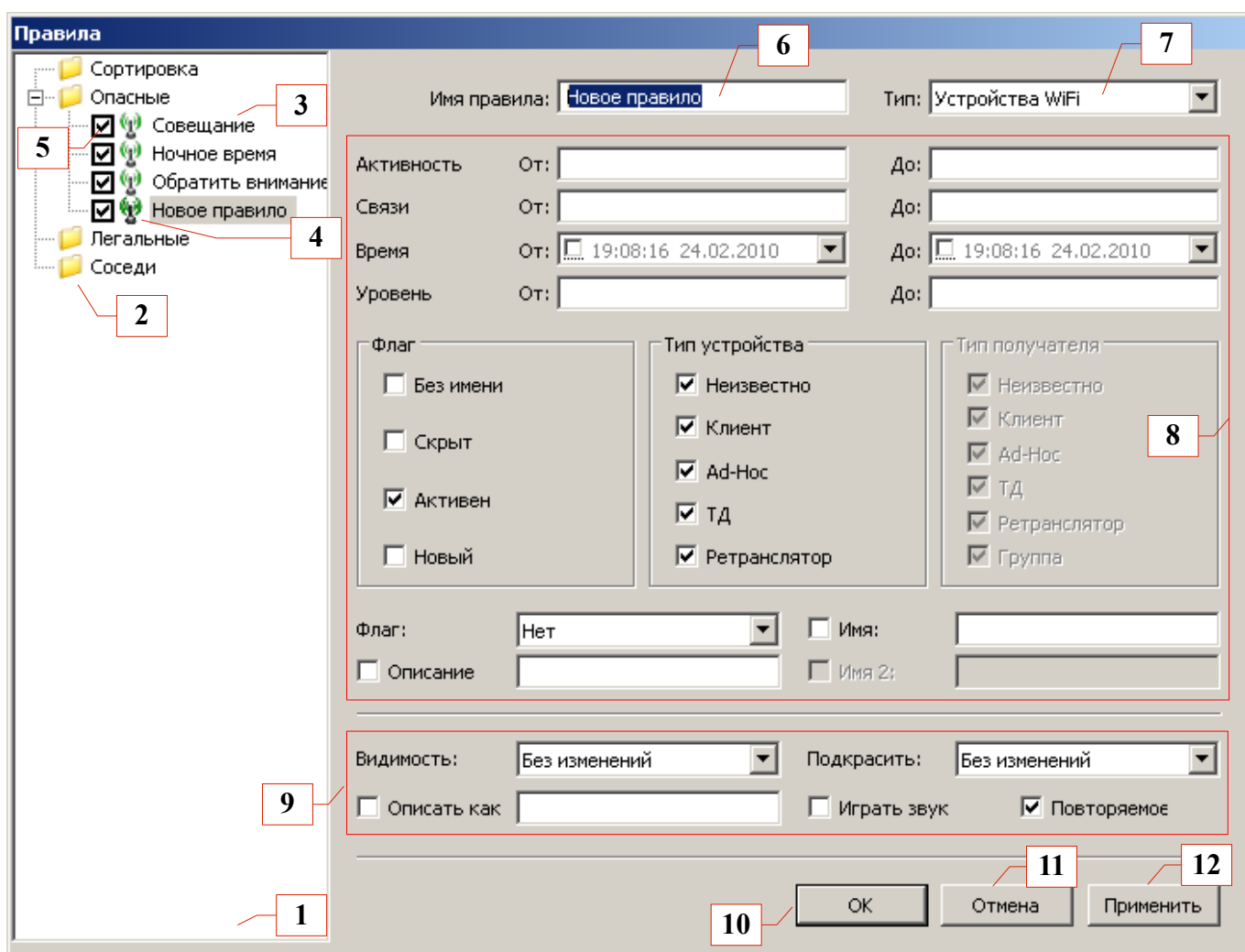


Рисунок 21 - Окно редактирования правил

12- кнопка Применить применяет изменения сделанные в правилах, сохраняет их, но не закрывает окно настроек.

9.3 Структура дерева правил

Правила в структуре сгруппированы по папкам. Рекомендуется однотипные правила размещать в одной папке. Новое правила можно создать только предварительно создав паку или выбрав одну из имеющихся папок. Нельзя расположить правило вне папки.

Новая папка создается из помощью контекстного меню правой кнопки мыши - Создать папку. После чего появиться диалоговое окно в котором необходимо ввести имя новой папки. Новая папка всегда добавляется в конец списка.

Папки в структуре не могут иметь одинаковые имена. При попытке создать папку с уже имеющимся именем будет выдано предупреждение.

Имена папок могут быть введены как латиницей так и кириллицей.

Папки можно открывать и сворачивать. Для этого необходимо кликнуть

по значку плюса (папка раскроется) или минуса (папка свернется).

Для того что бы переименовать паку выберите ее щелкнув по имени левой кнопкой мыши, после чего из контекстного меню правой кнопки мыши выберите пункт Переименовать папку. Появиться диалоговое окно с названием папки.

Для удаления папки выберите ее, кликнув по названию левой кнопкой мыши, после чего из контекстного меню правой кнопки мыши выберите пункт Удалить папку.



Все правила, которые находятся в папке будут удалены с ней.

9.4 Создание правила

Для создания нового правила выберите кликом левой кнопкой мыши папку для этого правила из существующей структуры или создайте новую папку. Из контекстного меню правой кнопки мыши выберите пункт Создать правило.

По умолчанию все правила называются «Новое». Для изменения названия правила наберите новое название в области названия.

Допускается одинаковые названия для правил в одной папке.

После ввода имени правила выберите его тип из списка.

9.5 Выбор условий Правила

Условия правила есть набор разведпризнаков по которым можно выделить объект с опасными признаками из общего списка автоматически. Условия правила формулируются в области ввода условий. Набор условий различается для правил различных типов. Выбор нужного набора осуществляется в поле «Тип».

9.5.1 Область ввода условий для устройств WiFi

Область ввода условий отбора объектов в окне Устройства состоит из полей:

The screenshot shows a configuration form for device rules. The fields are as follows:

- 1:** Text input for 'Имя правила' (Rule name), containing 'Новое правило'.
- 2:** Dropdown menu for 'Тип' (Type), set to 'Устройства WiFi'.
- 3:** Text input for 'Активность От:' (Activity start).
- 4:** Text input for 'Передано От:' (Transmitted data start).
- 5:** Text input for 'Принято От:' (Received data start).
- 6:** Time and date picker for 'Время От:' (Time start), set to 16:54:57 21.12.2010.
- 7:** Text input for 'Уровень От:' (Level start).
- 8:** Group of checkboxes for 'Состояние' (Status): 'Без имени', 'Скрыт', 'Активен' (checked), 'Новый', 'Невидимый'.
- 9:** Group of checkboxes for 'Тип устройства' (Device type): 'Неизвестно' (checked), 'Клиент' (checked), 'Ad-Нос' (checked), 'ТД' (checked), 'Ретранслятор' (checked).
- 10:** Dropdown menu for 'Флаг' (Flag), set to 'Нет'.
- 11:** Text input for 'Имя:' (Name).
- 12:** Text input for 'Имя 2:' (Name 2).

Рисунок 22 - Поля области ввода условий для устройств

- 1- Имя правила- поле позволяет определить название правила.
- 2- Тип определяет тип объекта для которого создано правило:
 - устройства WiFi
 - связи WiFi
 - устройства Bluetooth
 - устройства ZigBee
- 3- Активность — устанавливает интервал значений активностей устройств, которые удовлетворяют правилу.
- 4- Передано — устанавливает интервал значений объема суммарного исходящего трафика для устройства.
 Формат ввода поля:
 100 = 100 байт
 1.1k = 1.1 кбайт
 1.1M= 1.1 МБайт
- 5- Принято- устанавливает интервал значений объема суммарного

входящего трафика устройства.

Формат ввода поля:

100 = 100 байт

1.1k = 1.1 кбайт

1.1M = 1.1 МБайт

6- Время. Устанавливает интервал значений последней активности устройств, которые удовлетворяют правилу.



Порядок интерпретации условия с полями «От» и «До»

Если установлена галочка «От», но не установлена галочка «До», то будут выбраны все объекты списка, которые больше значения введенного в поле «От». Например, тип правила «Соединение» и данных от 10 Кб означает, что данному условию будут удовлетворять все соединения, объем переданных данных через которые превышает 10 Кб.

Если не установлена галочка «От», но установлена галочка «До», то будут выбраны все объекты списка, которые меньше значения введенного в поле «До». Например, тип правила «Устройства» и активность до 10 означает, что данному условию будут удовлетворять все устройства активность которых менее 10%.

Если галочки «От» и «До» установлены, то будут выбраны все значения таблицы, которые больше значения введенного в поле «От» и меньше значения введенного в поле «До». Например, тип правила «Соединение» и сессия от 10 до 30 означает, что данному условию будут удовлетворять все соединения, длительность которых больше 10, но меньше 30 минут.

Если значение в поле «От» превышает значение в поле «До» то правило будет применено к объектам за пределами интервала «От-До». Например, тип правила «Соединение» и сессия от 30 до 20 означает, что данному условию будут удовлетворять все соединения, длительность которых меньше 10, но больше 30 минут.

Если галочки «От» и «До» не установлены, то данные поля не используются даже если в них есть значения отличные от нуля.

7- Уровень — устанавливает интервал значений уровня сигнала, которые удовлетворяют правилу.

8- Состояние — определяет статус устройств, которые удовлетворяют правилу:

•Без имени — соответствует клиентам и точкам доступа у которых вместо имени стоит MAC адрес.

•Скрыт— соответствует всем скрытым устройствам

- Активен — соответствует всем активным устройствам.
- Новый — соответствует всем новым устройствам.



По умолчанию установлен выбор на атрибуте Активен.

9- Тип Устройства- определяет тип устройства (согласно полю Тип в списке Устройств) которое будет удовлетворять правилу:

- Неизвестное — устройство чей тип определить не удалось .
- Клиент — обычный клиент, устройство с иконкой.
- AdHoc —устройство в режиме клиент-клиент (AdHoc).
- Точка доступа — устройство в режиме обычной точки доступа.
- Ретранслятор — точка доступа в режиме ретранслятора.

По умолчанию выбраны все атрибуты, это означает что правило распространяется на все устройства независимо от атрибута.

10-Флаг — позволяет выбрать установленный флаг опасности устройств, которые удовлетворяют правилу.

- Нет— только устройства с пустым полем опасности
- Только легальные— только устройство с флагом .
- Только опасные — только устройства с флагом .
- Любые — все устройства независимо от флага.

11- Имя — позволяет отбирать только устройства с определенным в этом поле именем.

12- Описание — позволяет отбирать устройства только с определенными пользовательскими комментариями в поле описания списка Устройств. Условие работает только при полном совпадении данного поля с полем Описание в списке устройств.



Для активации условий «Имя» и «Описание» используется трехпозиционная галочка. Не активная галочка означает, что данное поле не используется, установленная галочка означает, что условию удовлетворяет совпадение введенной Пользователем строки с именем устройства. Пунктирная галочка означает, что условию удовлетворяет несовпадение введенной Пользователем строки с именем устройства.



Не забудьте поставить галочки при применении условий Имя и Описание. Без них условие работать не будет.

9.5.2 Область ввода условий для соединений WiFi

Область ввода условий отбора объектов в окне Соединения WiFi состоит из полей:

Имя правила: Новое правило Тип: Связи WiFi

% **1** От: До:

Данные **2** От: До:

Время **3** От: 14:09:09 27.02.2010 До: 14:09:09 27.02.2010

Уровень От: До:

4 **5** **6**

Флаг: **7** Нет Имя 1: **8**

Описание **10** Имя 2: **9**

Флаг: Без имени, Скрыт, Активен, Новый

Тип отправителя: Неизвестно, Клиент, Ad-Нос, ТД, Ретранслятор

Тип получателя: Неизвестно, Клиент, Ad-Нос, ТД, Ретранслятор, Группа

Рисунок 23 - Поля области ввода условий для соединений

1- % - устанавливает интервал значений поля % из списка Соединений, которые удовлетворяют правилу.

2- Данные — устанавливает интервал значений объема трафика данных переданных по соединению, который будет удовлетворять Правилу. Формат ввода поля:

100 = 100 байт

1.1k = 1.1 кбайт

1.1M = 1.1 МБайт

3- Время. Устанавливает интервал значений последней активности соединения, которые удовлетворяют правилу.



Порядок интерпретации условия с полями «От» и «До» аналогичен условиям для устройств.

4- Состояние — определяет статус соединений, которые удовлетворяют правилу, поле использует трехпозиционные галочки:

•Без имени — соответствует соединениям у которых вместо имени стоит MAC адрес отправителя. Третья позиция галочки означает выбор устройств у которых имя задано пользователем.

•Скрыт- соответствует всем скрытым соединениям вручную. Третья позиция - для не скрытых соединений.

•Активен — соответствует всем активным соединениям, в третьей позиции неактивным.

•Новый — соответствует всем новым соединениям или не новым в третьей позиции.

По умолчанию установлен выбор на атрибуте Активен.



5- Тип отправителя- определяет тип устройства отправителя (устройство имя которого стоит в названии соответствующей группы в окне Соединения) которое будет удовлетворять правилу:

- Неизвестное - устройство чей тип определить не удалось .
- Клиент — обычный клиент, устройство с иконкой.
- AdHoc- устройство в режиме клиент-клиент (AdHoc).
- Точка доступа - устройство в режиме обычной точки доступа.
- Ретранслятор - точка доступа в режиме ретранслятора.

По умолчанию выбраны все атрибуты, это означает что правило распространяется на все устройства независимо от атрибута.

6 — Тип получателя- определяет тип устройства получателя в связи. Выбор значений аналогичен отправителю.

7- Флаг — позволяет выбрать установленный флаг опасности соединения, которые удовлетворяют правилу.

- Нет- только связи с пустым полем опасности
- Только легальные- только связи с флагом .
- Только опасные — только связи с флагом .
- Любые— все связи независимо от флага.

8- Имя 1- позволяет отбирать только соединения с определенным именем отправителя.

9- Имя 2- позволяет отбирать только соединения с определенным именем получателя.

10- Описание- позволяет отбирать устройства только с определенными пользовательскими комментариями в поле описания списка Устройств. Условие работает только при полном совпадении данного поля с полем Описание в списке устройств.



Принцип работы трехпозиционных галочек в полях Имя и описание соответствует условиям для Устройств.



Не забудьте поставить галочки при применении условий Имя и Описание. Без них условие работать не будет.

9.5.3 Область ввода условий для устройств Bluetooth

Окно правил Bluetooth представлено на рисунке:

Правила

Bluetooth

Новое правило

Имя правила: Новое правило Тип: Устройства Bluetooth

Активность От: До:

Связи От: До:

Время От: 14:22:54 17.03.2010 До: 14:22:54 17.03.2010

Уровень От: До:

Состояние

Без имени

Скрыт

Активен

Новый

Невидимый

Тип устройства

Неизвестно

Клиент

Ad-Hoc

ТД

Ретранслятор

Тип получателя

Неизвестно

Клиент

Ad-Hoc

ТД

Ретранслятор

Группа

Флаг: Нет Имя:

Описание:

Имя 2:

Видимость: Без изменений Подчеркнуть: Без изменений

Описать как: Играть звук Повторяемое

ОК Отмена Применить

Рисунок 24: Окно ввода правил Bluetooth

Поля ввода условий для устройств Bluetooth аналогичны WiFi (**глава 9.5.1**), кроме:

- поля: Активность, Связи и Тип устройства недоступны;
- доступно поле «Невидимый». При выбранном поле «Невидимый» условие охватывает устройства Bluetooth, которые работают в невидимом режиме (подробнее см. **главу 10**).

9.5.4 Область ввода условий для устройств ZigBee

Окно правил ZigBee представлено на рисунке:

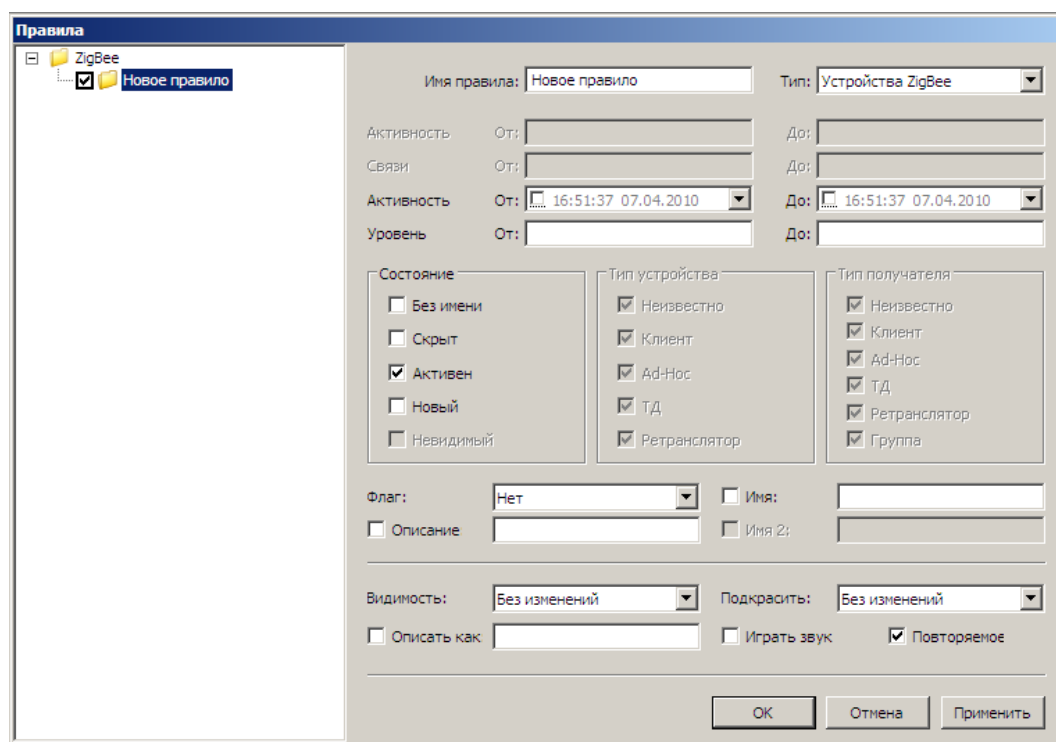


Рисунок 25: Окно ввода правил ZigBee

Поля ввода условий для устройств ZigBee аналогичны WiFi (**глава 9.5.1**), кроме:

- поля: Активность, Связи и Тип устройства недоступны.

9.6 Выбор действий для Правил

Выбор действий для устройств и соединений WiFi и устройство Bluetooth аналогичен.

Область ввода действий предназначена для определения действий, которые будут выполняться автоматически при выполнении всех условий заданных правилом. Эта область располагается непосредственно под условиями и состоит из следующих полей:

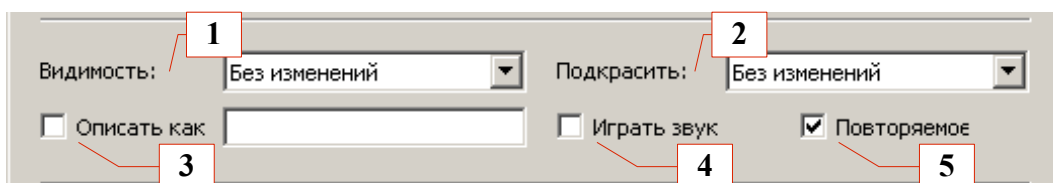


Рисунок 26- Область ввода действий

1- Видимость- позволяет автоматически изменять статус устройства/соединения на «Скрытый». При выборе действия «Показать», оно оставляет в списке только те устройства/соединения которые

удовлетворяют условиям Правила, а остальные скрывает.

При выборе «Скрыть», оно скрывает все устройства/соединения удовлетворяющие условиям Правила.



Действие «Показать» с условием «Активные» использовать не рекомендуется, поскольку это дублирует скрывание неактивных в настройках программы.

2- Подкрасить- позволяет автоматически изменить цвет строки с устройством/соединением, которое удовлетворяет условиям Правила. Значения поля:

- Без изменений оставляет цвет строки без изменений.
- Нет- удаляет окраску если она была.
- Зеленый
- Желтый
- Красный.

3- Описать как — позволяет автоматически изменить поле пользовательских комментариев в списке Устройств.



Поле описание будет заменено и старое описание, если оно было в поле Описания до замены будет уничтожено.



Не забудьте поставить галочки рядом с действием «Описать как». Без галочки действие работать не будет.

4-Играть звук- позволяет проигрывать звуковой файл при срабатывании Правила.



При срабатывании большого количества правил, предусматривающих подзвучку, происходит лавинообразное звуковое сопровождение, во избежание чего рекомендуем использовать данное свойство в правилах, предполагающих одиночное срабатывание.

5- Повторяемое. Если в поле «Повторяемое» нет галочки правило срабатывает однократно :

- При нажатии кнопок «Применить» или «Ок».
- При обновлении любого поля у устройства/соединения в списке.
- При приходе любого пакета от/к устройству.

9.7 Работа с правилами в режиме сканирования

Работа с правилами во время сканирования происходит в автоматическом режиме. При этом, проверяются все активные правила (с установленной галочкой в поле выбора рядом с названием Правила).

10 Поиск «невидимых» устройств Bluetooth.

Устройства Bluetooth могут находиться в режиме «невидимый» (hidden mode). В этом режиме устройство не отвечает на запросы и не обменивается информацией. Для обнаружения устройства в режиме «невидимый» необходимо, что бы оно хотя бы раз было обнаружено в режиме «активный» или необходимо знать его MAC адрес.

Соответственно, существуют две возможности обнаружить устройство в «неактивном» режиме:

•если в списке есть такое устройство, то оно скорее всего будет иметь статус «неактивный». Для выявления устройств находящихся в режиме «невидимый», необходимо выбрать это устройство в списке (галочка в поле Выбор) и из меню правой кнопки мыши выбрать пункт Опросить\Выбранные.

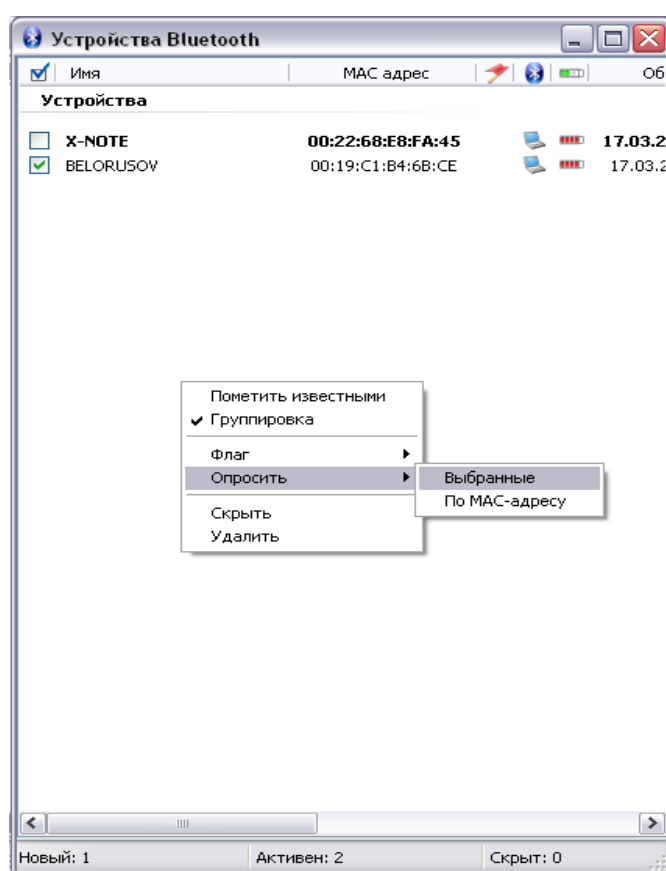



Рисунок 27: Опрос Bluetooth устройств по списку

Если для одного или нескольких выбранных устройств будет обнаружен отклик, рядом с именем устройства появится значок , который означает, что устройство работает в невидимом режиме.

•второй способ обнаружить «невидимые» Bluetooth устройства- опросить

по MAC адресу. Из меню правой кнопки мыши команда Опросить\По MAC адресу

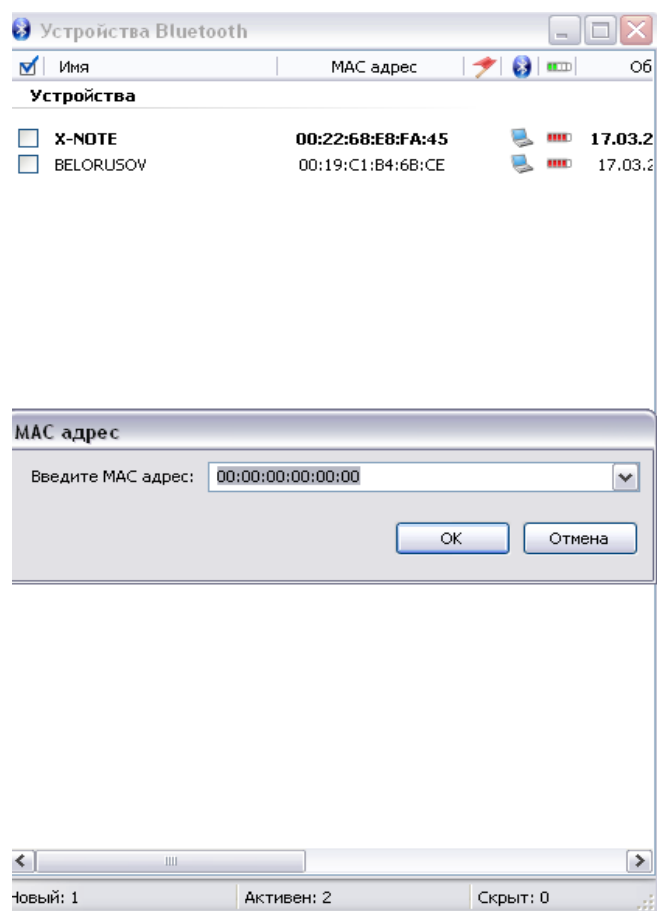




Рисунок 28: Опрос по MAC адресу

В появившемся окне следует указать MAC устройства. Если для одного будет обнаружен отклик, устройство появится в списке и рядом с именем устройства появится значок , который означает, что устройство работает в «невидимом» режиме.



Включенное правило Невидимые для устройств Bluetooth позволяет автоматически подкрашивать строчки с обнаруженными устройствами Bluetooth с закрытым режимом красным цветом. Но следует иметь в виду, что если удалить из списка вручную устройство, которое работает в открытом режиме, и после этого опросить его по MAC адресу, то на нем так же сработает правило Невидимые.

11 Отчет

Программа позволяет автоматически создавать отчет результатов работы. Отчет можно создать с помощью кнопки  на Панели инструментов или с помощью команды Инструменты-Отчет.

При сохранении имеется возможность выбрать формат *.txt (текстовый файл) или *.csv (OpenOffice Calc) и возможность выбора места хранения отчета (по умолчанию все отчеты сохраняются в папке /opt/zodiac/reports).



Для просмотра файлов *.csv должно быть установлено приложение OpenOffice Calc.

Сохраненный отчет автоматически открывается в отдельном окне в соответствующем редакторе.

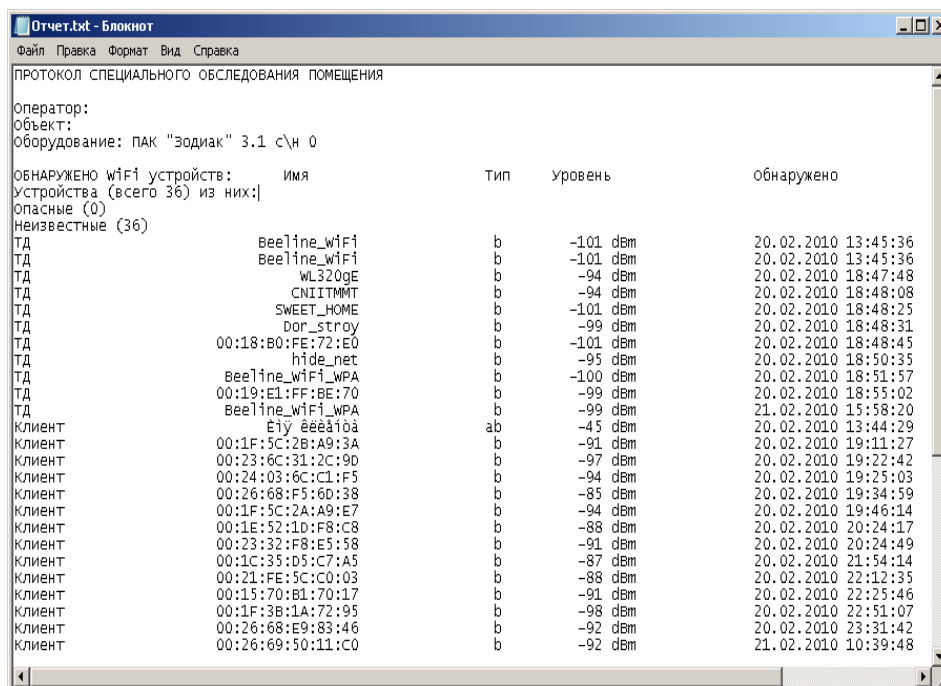


Рисунок 29: Отчет в формате txt

В отчет помещается информация только о видимых объектах списка устройств, объекты, скрытые правилами в отчет не помещаются, объекты, скрытые системными настройками в отчет помещаются.



Если требуется не помещать в отчет, например, неактивные устройства, то их необходимо скрыть в списках соответствующим

правилом, а не через системные настройки «скрывать неактивные».

В отчете сохраняется информация о количестве обнаруженных устройств WiFi и Bluetooth, а так же расширенная информация по всем опасным (флаг Опасный) и неизвестным (без флага) устройствам. Расширенная информация содержит поля: Имя, Уровень, Суммарный объем трафика данных переданных этим устройством, Описание.

По легальным устройствам (флаг Легальный) указывается только их количество, а расширенная информация в отчете не приводится.



В поле «Данные» в отчете приводится суммарный трафик по всем получателям которым данное устройство передавало информации. Соответственно значение в этом поле может отличаться от значение поля Данные в списке связей для одной связи этого устройства.

12 Методические рекомендации.

12.1 Полезные советы

Некоторые WiFi устройства в целях энергосбережения могут работать в следующем режиме: при включении устройство активно, если в течении какого то периода времени (от 30 секунд до 1 минуты) устройство не устанавливает соединение, то оно переходит в режим энергосбережения и становится неактивным. Через несколько минут оно опять становится активным и так далее. Если в настройках интервал неактивности установлен в 60 сек. а период активности устройства менее минуты, то возможна ситуация когда устройство отображается в списке всегда как активное (не успевает сменить статус), а поле Сеанс всегда имеет значение 0- потому что длительность любого сеанса указывается в минутах.

Среди широковещательных точек доступа могут встречаться «скрытые» - это нормальная ситуация. Эти точки доступа держаться оператором в резерве и имеют статус «скрытый», что бы к ним не было обращений пока они в резерве.

13 Паспорт

- СПО «ЗОДИАК про»
серийный номер _____

- ПЭВМ
серийный номер _____

- WiFi адаптер
IEEE 802.11 a b g n
 мультирежим
 встроенный
 внешний
 серийный номер _____

- Bluetooth адаптер
встроенный
 внешний
 BT-11
 серийный номер _____

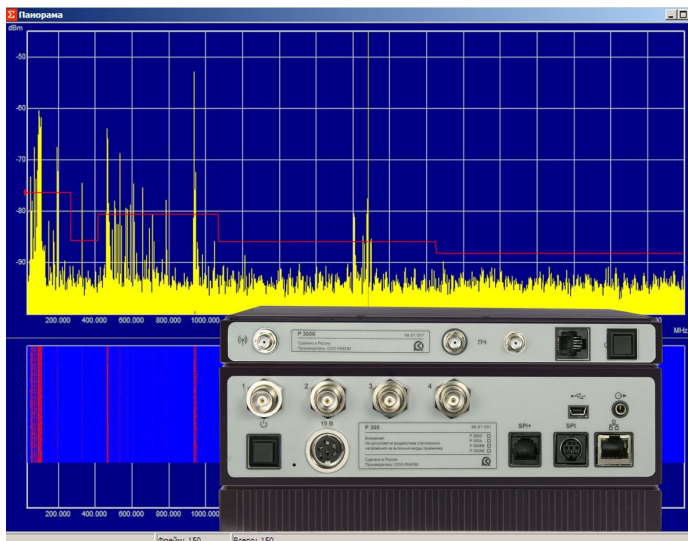
- ZigBee адаптер
ZB-11
 серийный номер _____

Дата выпуска _____

ОТК _____ МП

ЭВРИКА

Автоматизированный комплекс радиоконтроля, который разработан специально для выявления несанкционированных радиопередатчиков в защищаемых помещениях.



Аппаратная часть комплекса основана на панорамном приемнике P300. Это позволяет сканировать частотный диапазон шириной 3 ГГц всего за несколько секунд и анализировать сигналы в реальном масштабе времени в полосе до 52 МГц.

ЭВРИКА предлагает оператору абсолютно новый подход к обработке радиосигналов, который основан на специально разработанной реляционной базе данных. База данных обеспечивает оператору быстрый доступ к необходимой информации о сигналах, связанных с ними архивных данных и эталонными образцами. База данных автоматически сортирует сигналы по разведпризнакам и делает процесс обнаружения «подозрительных» сигналов быстрым и эффективным.

Оператор, сравнивая полученные данные с библиотекой эталонных образцов, которые постоянно обновляются разработчиком, может быстро и точно определить тип несанкционированного радиопередатчика.

В комплексе доступен широкий набор инструментов для технического анализа сигналов – анализатор спектра и осциллограф, векторный анализатор, водопад и маркерные измерения. Уникальной особенностью комплекса является возможность исследовать сигнал сразу во всех анализаторах одновременно.

Важным преимуществом комплекса является возможность ручной и автоматической записи сигнала. Записанных массив комплексных данных позволяет оператору полностью восстановить исходный сигнал для доследования в любом анализаторе которые доступны в комплексе, даже если этого сигнала уже нет в эфире.

Возможности ЭВРИКИ могут легко наращиваться: от базовой до экспертной версии. Дополнительные возможности экспертной версии:

- Полосы анализа сигнала до 26 МГц
- Сетевая конфигурация
- Дополнительные инструменты технического анализа
- Инструменты планирования заданий
- Дополнительные настройки аппаратной части

Подробную информацию и демонстрационную версию программного обеспечения можно получить на сайте www.rusmonitor.ru