



**Закрытое Акционерное Общество
"Научно производственное объединение РТК"**

УТВЕРЖДЕН

54323649.508100.00001-0134-ЛУ

**ПРОГРАММНЫЙ КОМПЛЕКС
АНАЛИЗАТОР ФАЙЛОВ РЕГИСТРАЦИИ ССПТ-1М**

Руководство оператора
54323649.508100.00001-0134

Инв. № подл.	Подп. и дата	Взам.инв.№	Инв. № дубл.	Подп. и дата

Санкт-Петербург

2006

© ЗАО "НПО РТК", 2002 - 2006.

Тихорецкий пр., д. 21. Санкт-Петербург. 194064. Российская Федерация

Телефон/Факс: +7 (812)-552-4512

E-mail: info@npo-rtc.ru WWW: <http://www.npo-rtc.ru>

№ изм.	Подпись	Дата

АННОТАЦИЯ

Настоящее руководство описывает назначение, область применения, общие принципы функционирования, порядок установки и управления программным комплексом «Анализатор файлов регистрации ССПТ-1М» и предназначено для специалистов в области сетевой безопасности и администраторов сетей, использующих межсетевой экран ССПТ-1М для решения вопросов, связанных с ограничением доступа к информационным и сетевым ресурсам в сетях Ethernet.

Программный комплекс «Анализатор файлов регистрации ССПТ-1М» поставляется на компакт-диске в комплекте с настоящим руководством.

№ изм.	Подпись	Дата

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ	5
1.1. Назначение и область применения комплекса «Анализатор файлов регистрации ССПТ-1М»	5
1.2. Описание комплекса «Анализатор файлов регистрации ССПТ-1М» и принципов его функционирования.....	6
2. СИСТЕМНЫЕ ТРЕБОВАНИЯ.....	9
3. УСТАНОВКА КОМПЛЕКСА «АНАЛИЗАТОР ФАЙЛОВ РЕГИСТРАЦИИ ССПТ-1М»	10
3.1. Настройка сервера FTP в Windows XP	10
3.2. Установка и удаление комплекса «Анализатор файлов регистрации ССПТ-1М»	14
4. ИНТЕРФЕЙС ОПЕРАТОРА	19
4.1. Главное окно	19
4.2. Команды меню.....	21
4.2.1. Меню “Файл”	21
4.2.2. Меню “Вид”	28
4.2.3. Меню “Сервис”	29
4.2.4. Меню “Справка”	34
4.3. Параметры построения диаграммы	35
5. ФОРМАТЫ ТАБЛИЦ	36
6. К СВЕДЕНИЮ АДМИНИСТРАТОРОВ.....	41

№ изм.	Подпись	Дата

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область применения комплекса «Анализатор файлов регистрации ССПТ-1М»

«Анализатор файлов регистрации ССПТ-1М» применяется в информационных системах, использующих в качестве средства защиты информации от несанкционированного доступа межсетевые экраны ССПТ-1М (54323649.401350.003 ТУ).

Программный комплекс «Анализатор файлов регистрации ССПТ-1М» предназначен для приема, преобразования, отображения и анализа информации о событиях, происходящих в процессе работы межсетевого экрана и пакетах, проходящих через фильтрующие интерфейсы ССПТ-1М.

«Анализатор файлов регистрации ССПТ-1М» обеспечивает выполнение задач сбора, обработки и визуализации информации, зарегистрированной и переданной ССПТ-1М на внешний FTP-сервер.

Программа выполняет следующий набор функций:

- открытие базы данных
- осуществление запроса к базе данных;
- фильтрация загружаемой информации по заданным критериям;
- сохранение обработанной информации в файлах форматов: Текстовые файлы (*.txt), HTML файлы (*.htm), CSV (XLS) файлы (*.csv), XML файлы (*.xml), RTF файлы (*.rtf);
- выведение полученной из базы данных информации в структурированную таблицу или диаграмму.

№ изм.	Подпись	Дата

1.2. Описание комплекса «Анализатор файлов регистрации ССПТ-1М» и принципов его функционирования

«Анализатор файлов регистрации ССПТ-1М» состоит из двух подсистем (рис.1.1):

- **Подсистема конвертации и хранения.** Данная подсистема реализована в виде сервиса Windows, который осуществляет конвертацию бинарных файлов и распределение записей о пакетах и событиях по таблицам (TCP, UDP, ICMP, IP, ETH, ARP, IPX, СОБЫТИЯ). После обработки принятые бинарные файлы удаляются;

- **Подсистема визуализации.** Данная подсистема реализована в виде графического интерфейса для работы с базой данных, в котором можно производить запросы и сохранять полученные отчеты.

Структура комплекса «Анализатор файлов регистрации ССПТ-1М»

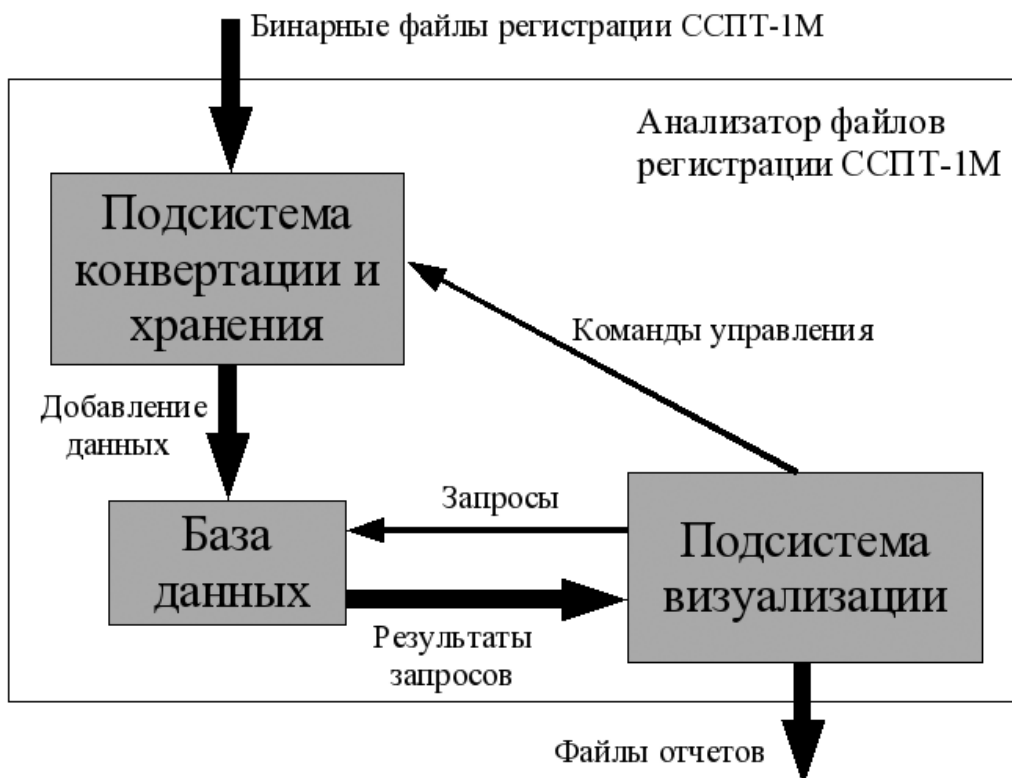


Рис. 1.1

№ изм.	Подпись	Дата

Каждая из подсистем представляет собой отдельное приложение. Данные приложения взаимодействуют между собой при помощи передачи сообщений.

Подсистема конвертации и хранения регистрируемой информации межсетевого экрана ССПТ-1М выполняет:

- конвертацию файлов регистрации ССПТ-1М из бинарного формата в текстовый и затем в формат SQL-запроса для добавления данных в таблицы;
- распределение полученных данных по таблицам;
- контроль количества записей в таблицах;
- контроль изменения суток;
- архивирование базы данных;
- контроль ввода команд администратора (архивация БД, старт, стоп);
- контроль изменения администратором параметров подсистемы (путь к папке с бинарными файлами, предельное количество записей в таблицах, ежесуточная архивация, период времени хранения архивов, контроль общего количества записей во всех таблицах);
- ведение протокола работы.

Данные, используемые при работе комплекса «Анализатор файлов регистрации ПО ССПТ-1М», хранятся в базе данных, управляемой СУБД SQLite. База данных содержит таблицы с информацией о зарегистрированных пакетах; таблицу с информацией о событиях, происходящих на межсетевых экранах; таблицу со статистической информацией о зарегистрированных пакетах; таблицу с описанием параметров межсетевых экранов, информация от которых хранится в базе данных.

В процессе взаимодействия подсистемы конвертации и хранения с базой данных можно выделить следующие этапы:

- открытие базы данных. При запуске осуществляется открытие файла базы данных;

№ изм.	Подпись	Дата

- подготовка SQL-запросов для добавления данных в таблицы. После конвертации бинарного файла осуществляется формирование SQL-запросов для добавления полученных данных в различные таблицы, в зависимости от протокола;
- открытие транзакции; Открытие и закрытие транзакции необходимо для увеличения быстродействия и соблюдения целостности данных;
- выполнение QSL-запросов добавления данных;
- закрытие транзакции;
- закрытие базы данных. При останове системы осуществляется закрытие базы данных.

Основной задачей подсистемы визуализации является отображение информации о зарегистрированных пакетах в виде табличных отчётов, а также построение графического представления данных. Подсистема визуализации является однопоточным приложением, функциональность которого инкапсулирована в классе LogProcessorApp, реализованного на основе стандартного класса приложения wxApp.

Подсистема визуализации выполняет:

- выборку из базы данных необходимой пользователю информации;
- отображение данных в виде настраиваемых таблиц;
- группировку информацию в сессии.

Подсистема визуализации осуществляет передачу следующих сообщений подсистеме конвертации и хранения:

- Старт;
- Стоп;
- Архивация БД;
- Изменение параметров.

№ изм.	Подпись	Дата

2. СИСТЕМНЫЕ ТРЕБОВАНИЯ

«Анализатор файлов регистрации ССПТ-1М» устанавливается на компьютер, тактовая частота процессора которого должна быть не менее 2000 МГц. Объем оперативной памяти должен быть не менее 512МБ. Компьютер должен быть укомплектован монитором и устройствами ввода (клавиатура и «мышь»). На компьютере должна быть установлена операционная система Windows XP или Windows Server 2003.

Размер необходимого свободного дискового пространства зависит от объемов трафика проходящего через межсетевой экран, настроек анализатора файлов регистрации и настроек правил в межсетевом экране. Например: Объем регистрируемой межсетевым экраном ССПТ-1М информации, при включении регистрации на всех глобальных правилах и при максимальной нагрузке достигает следующих значений: за 30 минут работы было выгружено 3 000 000 записей (на диске этот объем занимает 900 Мб). Под максимальной нагрузкой понимается трафик проходящий через межсетевой экран при использовании программы тестирования пропускной способности IPERF (<http://dast.nlanr.net/Projects/Iperf/>).

Вы можете провести тестирование в вашей сети и подсчитать, какой объем будет занимать база данных при ваших настройках регистрации, в зависимости от этого примите решение о том, сколько необходимо свободного дискового пространства. Рекомендуемый объем свободного дискового пространства – не менее 160 ГБ.

№ изм.	Подпись	Дата

3. УСТАНОВКА КОМПЛЕКСА «АНАЛИЗАТОР ФАЙЛОВ РЕГИСТРАЦИИ ССПТ-1М»

Для начала обработки файлов регистрации необходимо выполнить следующие операции.

На управляющем компьютере:

- настроить и запустить FTP-сервер;
- настроить и запустить «Анализатор файлов регистрации ССПТ-1М».

На межсетевом экране:

- включить в необходимых правилах регистрацию пакетов;
- включить выгрузку файлов регистрации.

Операции по настройке межсетевого экрана необходимо проводить в соответствии с Руководством администратора, входящем в комплект поставки ССПТ-1М.

3.1. Настройка сервера FTP в Windows XP

Служба FTP зависит от служб IIS (Internet Information Services). Чтобы установить службы IIS и FTP, выполните следующие действия.

В Windows XP служба FTP не устанавливается по умолчанию. Воспользуйтесь для установки службы FTP компонентом «Установка и удаление программ» панели управления.

1. В меню **Пуск** выберите пункт **Панель управления** и запустите компонент **Установка и удаление программ**.

2. Выберите кнопку **Установка компонентов Windows**.

3. В списке **Компоненты Windows** (рис.3.1) выберите пункт **Internet Information Service (IIS)** и выберите кнопку **Состав** (рис.3.2).

4. Установите флажок **File Transfer Protocol (FTP) Service**.

5. Выберите кнопку **Далее**.

№ изм.	Подпись	Дата

Окно Мастер компонентов Windows

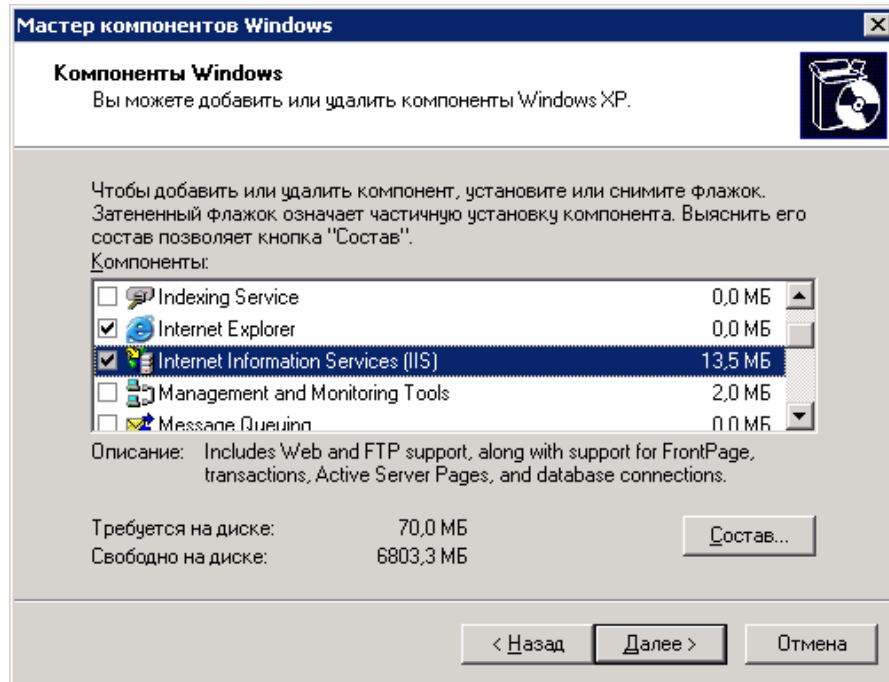


Рис.3.1

Окно Internet Information Service(IIS)

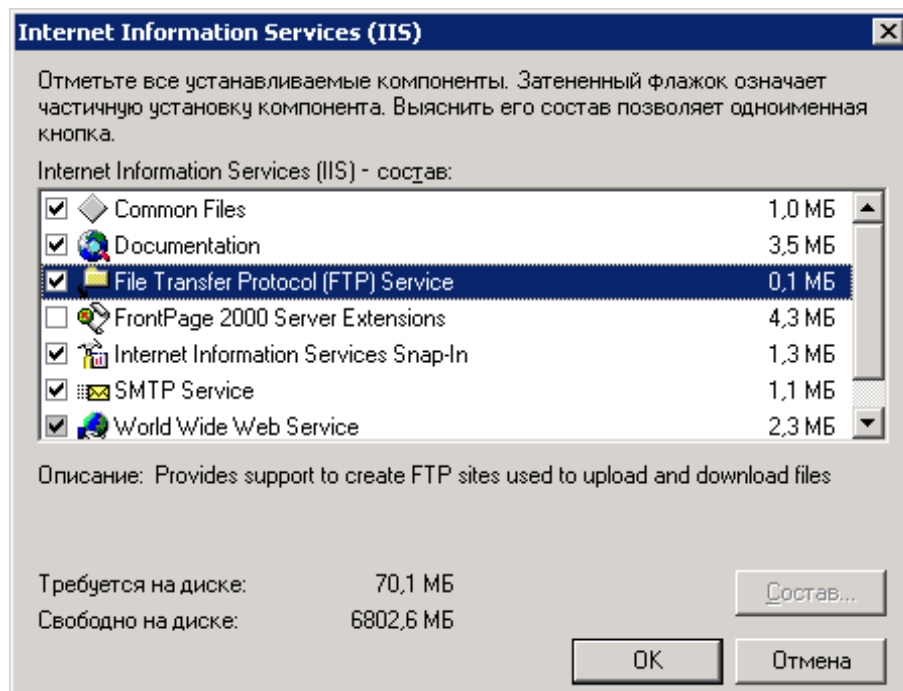


Рис.3.2

№ изм.	Подпись	Дата

7. В ответ на соответствующий запрос вставьте компакт-диск Windows XP или укажите путь к месту расположения файлов и выберите кнопку **ОК**.

8. Выберите кнопку **Готово**.

Службы IIS и FTP будут установлены. Перед началом использования службы FTP ее необходимо настроить.

Чтобы настроить службу FTP на прием подключений, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Панель управления** затем **Администрирование** и запустите **Internet Information Services** .

2. Разверните компонент **Узлы FTP** (рис.3.3).

Окно Internet Information Services

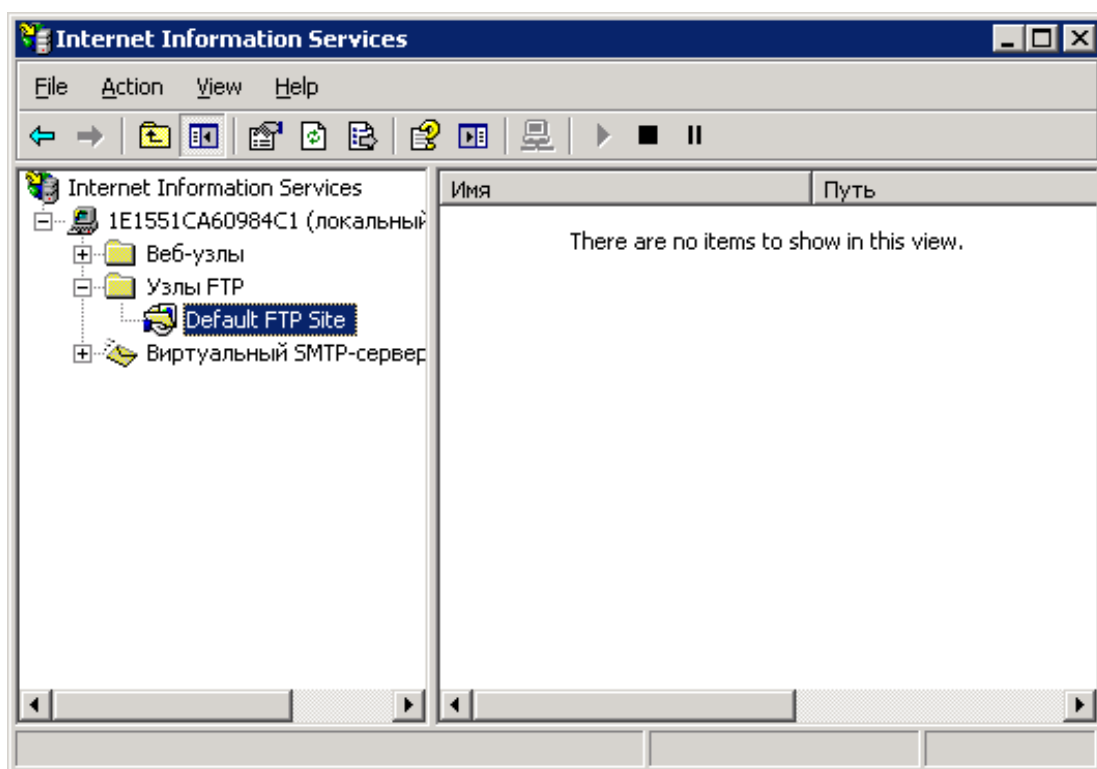


Рис.3.3

3. Выберите элемент FTP-узел по умолчанию и пункт **Свойства**.

4. Перейдите на вкладку **Безопасные учетные записи** (рис.3.4).

№ изм.	Подпись	Дата

5. Уберите флажок **Разрешить анонимные подключения** и флажок **Разрешить только анонимные подключения**.

6. Перейдите на вкладку **Домашний каталог** (рис.3.5).

8. Установите флажки **Чтение** и **Запись** и выберите стиль вывода каталогов Unix.

9. Выберите кнопку **ОК**.

10. Закройте диспетчер служб IIS или оснастку IIS.

11. В Windows создайте учетную запись с паролем под которой межсетевой экран будет выгружать по FTP файлы регистрации.

Безопасные учетные записи

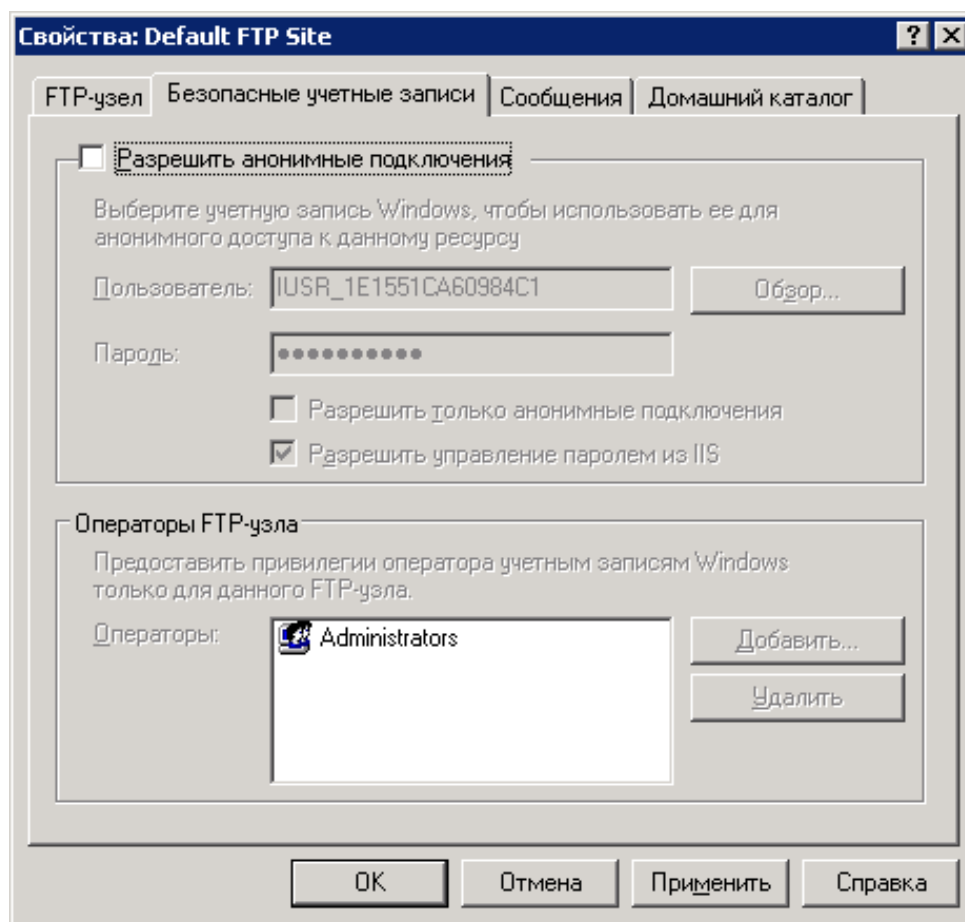


Рис.3.4

№ изм.	Подпись	Дата

Домашний каталог

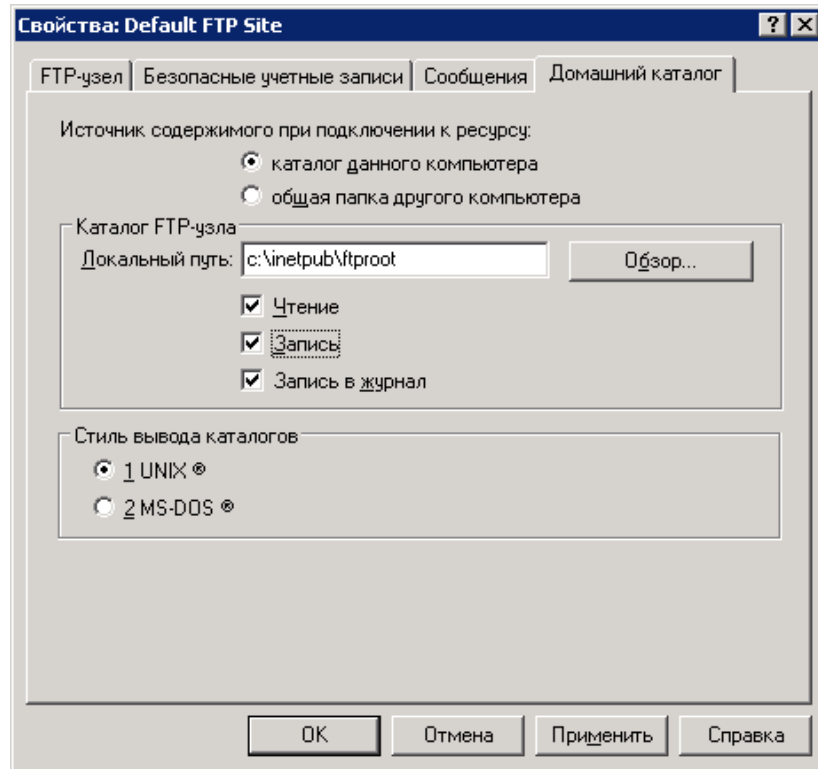


Рис.3.5

Сервер FTP готов принимать входящие запросы FTP. По умолчанию используется папка c:\inetpub\ftproot, где диск c - это диск, на котором установлены службы IIS.

3.2. Установка и удаление комплекса «Анализатор файлов регистрации ССПТ-1М»

Для установки анализатора файлов регистрации ССПТ-1М необходимо запустить программу установщик fnplog-setup.exe.

Откроется окно представленное на рисунке 3.6.

Необходимо выбрать «Далее» для продолжения установки. После этого откроется окно для выбора компонентов устанавливаемой программы (рис.3.7).

№ изм.	Подпись	Дата

Окно установки Анализатора файлов регистрации ССПТ-1М

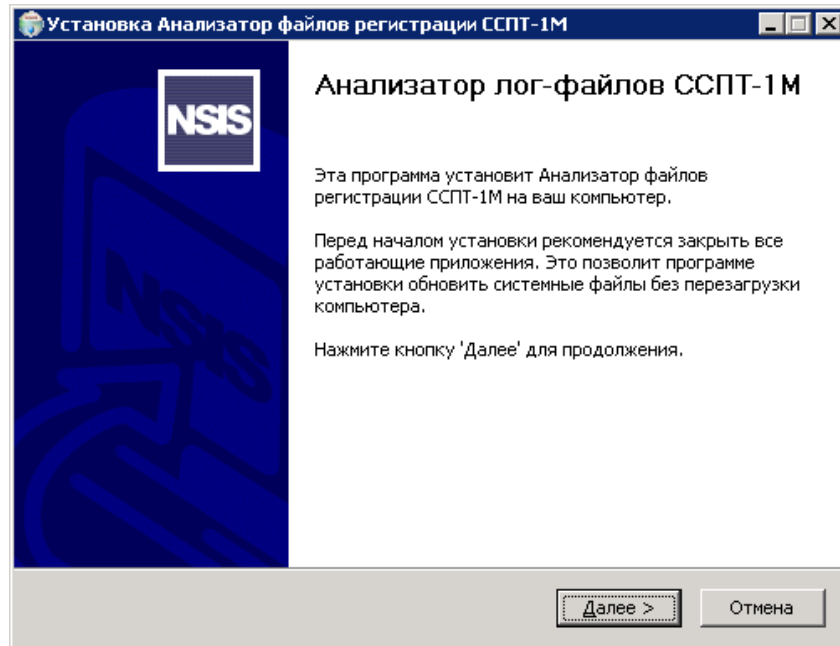


Рис.3.6

Окно выбора компонентов устанавливаемой программы

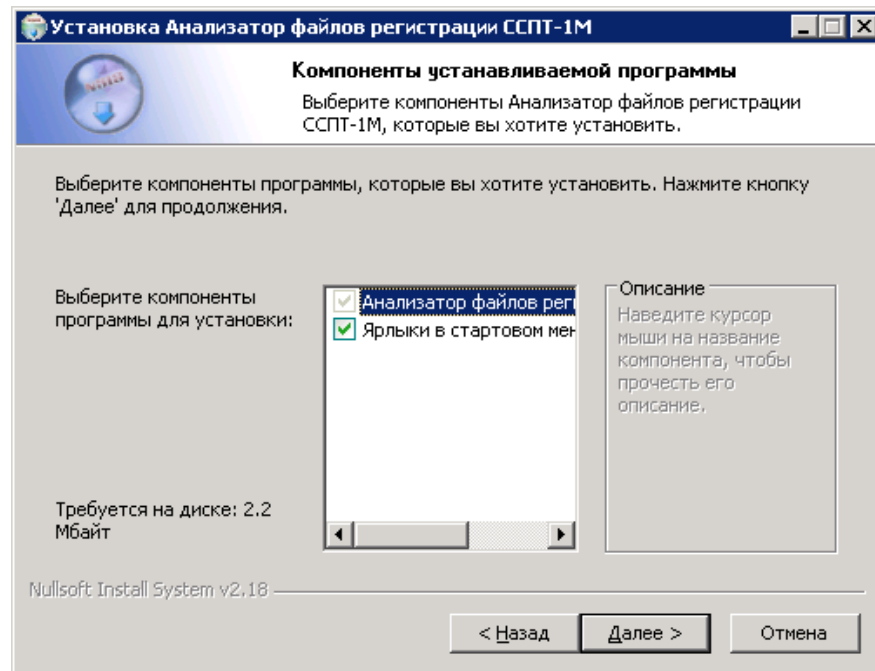


Рис.3.7

№ изм.	Подпись	Дата

Необходимо выбрать «Далее» для продолжения установки. После этого откроется окно для выбора папки установки (рис.3.8).

Окно выбора папки

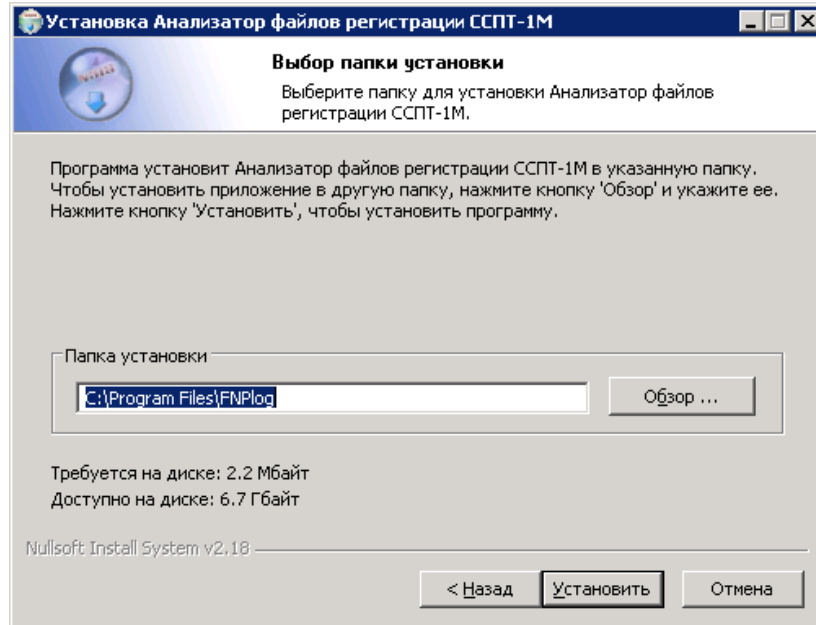


Рис.3.8

Для продолжения установки необходимо выбрать «Далее». После этого будет осуществлена запись файлов программы в выбранную папку и показано окно завершения установки (рис.3.9).

Окно завершения установки

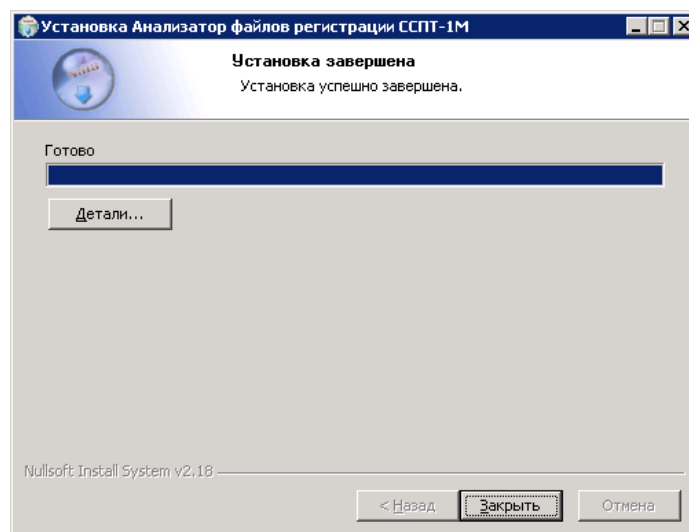


Рис.3.9

№ изм.	Подпись	Дата

Для удаления Анализатора файлов регистрации ССПТ-1М нужно запустить из меню «Пуск» - «Программы» - «Анализатор файлов регистрации ССПТ-1М» программу «Удаление» или из папки программы файл **uninstall.exe**. После этого будет отображено окно программы удаления (рис.3.10).

Окно удаления Анализатора файлов регистрации ССПТ-1М

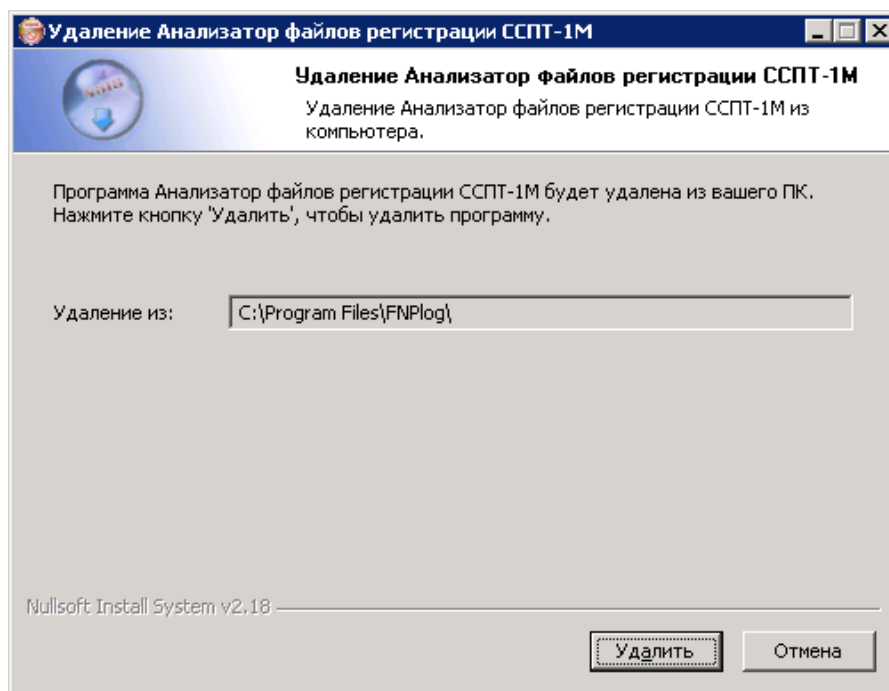


Рис.3.10

Для продолжения удаления необходимо нажать «Удалить». Начнется процесс удаления и будет показан диалог (рис.3.11), в котором можно выбрать удалять файлы базы данных и шаблоны запросов или нет.

После этого будет показано окно завершения удаления (рис.3.12).

№ изм.	Подпись	Дата

Окно запроса при удалении Анализатора файлов регистрации ССПТ-1М

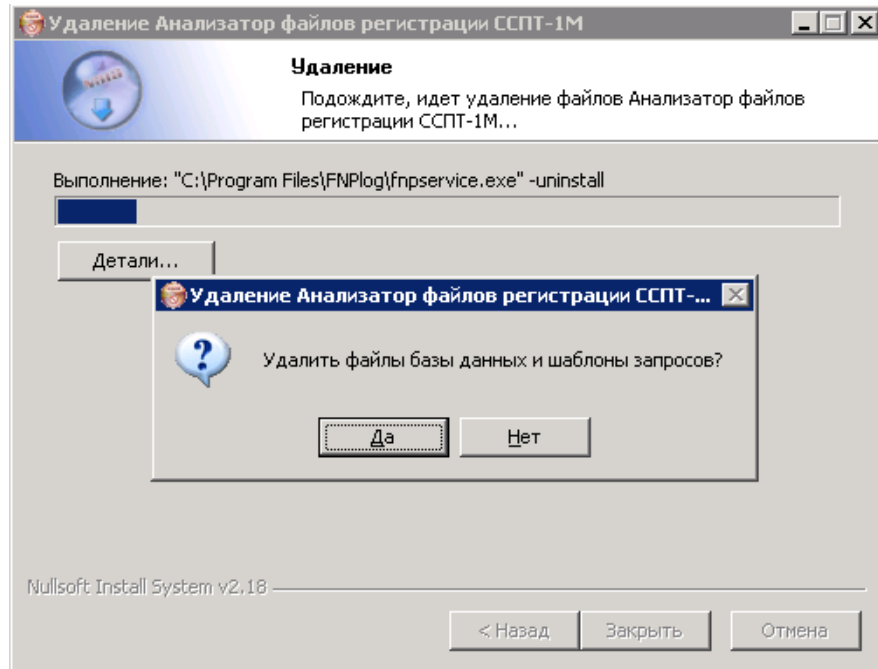


Рис.3.11

Завершение удаления Анализатора файлов регистрации ССПТ-1М

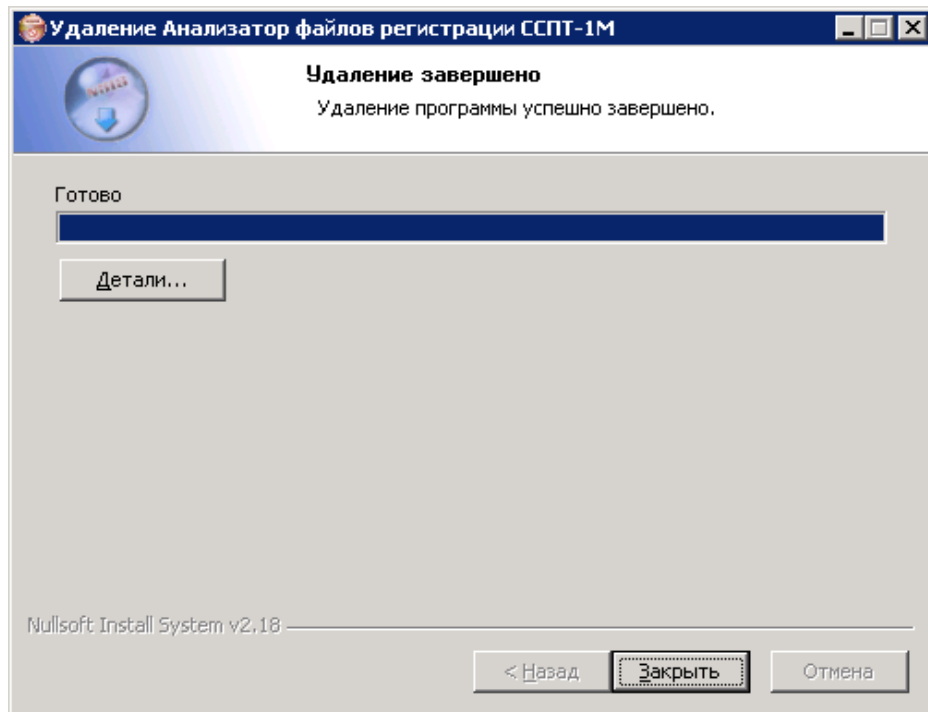


Рис.3.12

№ изм.	Подпись	Дата

4. ИНТЕРФЕЙС ОПЕРАТОРА

4.1. Главное окно

Главное окно (рис.4.1) состоит из следующих функциональных частей:

- меню;
- панель инструментов;
- верхнее окно - таблица сессий;
- нижнее окно - таблица ,в которой отображаются пакеты при раскрытии сессий;
- клавиши управления отображением (предыдущие/следующие сессии/пакеты);
- статусная строка.

Главное окно

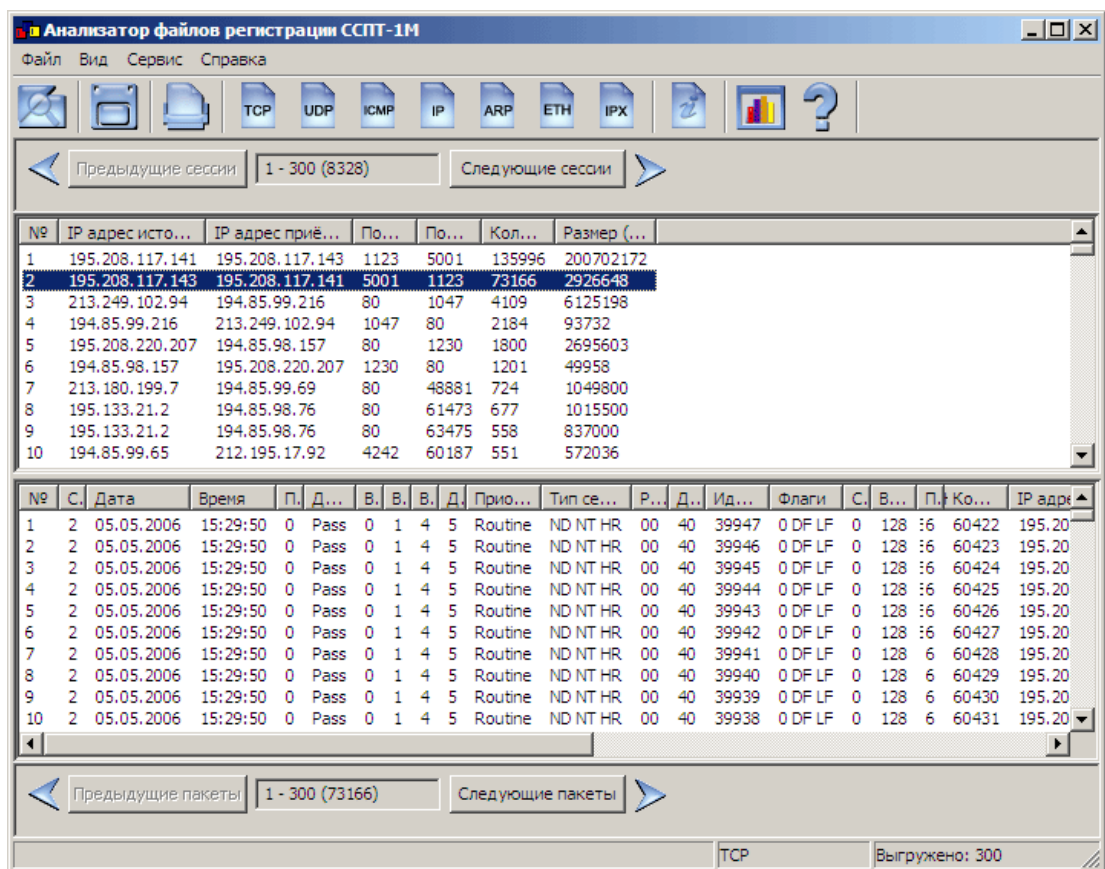


Рис.4.1

№ изм.	Подпись	Дата

Под сессией в данном случае понимается результат группировки значений при выборке из базы данных, согласно заданным полям группировки.

Например: Если для протокола ip_tcp заданы поля группировки: ip-адрес источника, ip-адрес приемника, порт источника и порт приемника, то в процессе обработки запроса будут найдены все записи с одинаковыми заданными полями и в списке сессий будет отображено содержимое этих полей, количество найденных пакетов и размер сессии (Вычисляется только для тех протоколов, где в формате присутствует поле размер). При двойном щелчке по сессии в нижнем окне будут отображены все пакеты, которые входят в эту сессию (раскрытие сессии).

Панель инструментов содержит следующие элементы:



- Создать запрос. Открывается диалог **Запрос к базе данных**.



- Экспорт данных. Открывается диалог для **выбора экспортируемых данных**.



- Печать. Открывается диалог печати.



- Производится запрос и в списке сессий отображаются данные по протоколу **TCP**.



- Производится запрос и в списке сессий отображаются данные по протоколу **UDP**.



- Производится запрос и в списке сессий отображаются данные по протоколу **ICMP**.





- Производится запрос и в списке сессий отображаются данные по протоколу **IP**.



- Производится запрос и в списке сессий отображаются данные **ARP/RARP**.

№ изм.	Подпись	Дата

 - Производится запрос и в списке сессий отображаются данные по кадрам **ETH**.

 - Производится запрос и в списке сессий отображаются данные по протоколу **IPX**.

 - Производится запрос и в списке сессий отображаются **События**.

 - Открывается диалог **Параметры построения диаграммы**.

 - Открывается Справка.

4.2. Команды меню

4.2.1. Меню “Файл”

Меню файл (рис.4.2) содержит следующие команды.

Меню файл

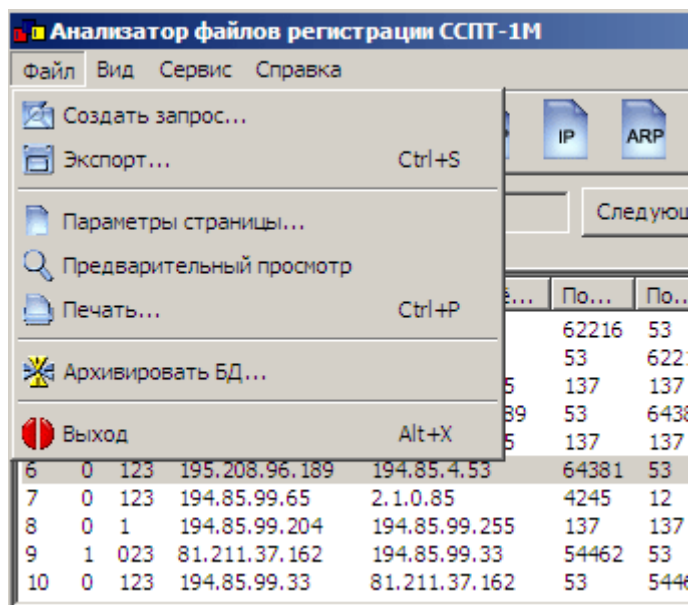


Рис.4.2

Создать запрос - Создать запрос к базе данных. Открывается форма (рис.4.3) для ввода параметров запроса. В этой форме можно задать период времени для выборки и выбрать межсетевой экран. Также можно сохранить

№ изм.	Подпись	Дата

шаблон запроса в выбранном файле, выбрать сохраненный шаблон и изменить параметры выборки, чтобы создать специфичный запрос.

Окно запроса к базе данных

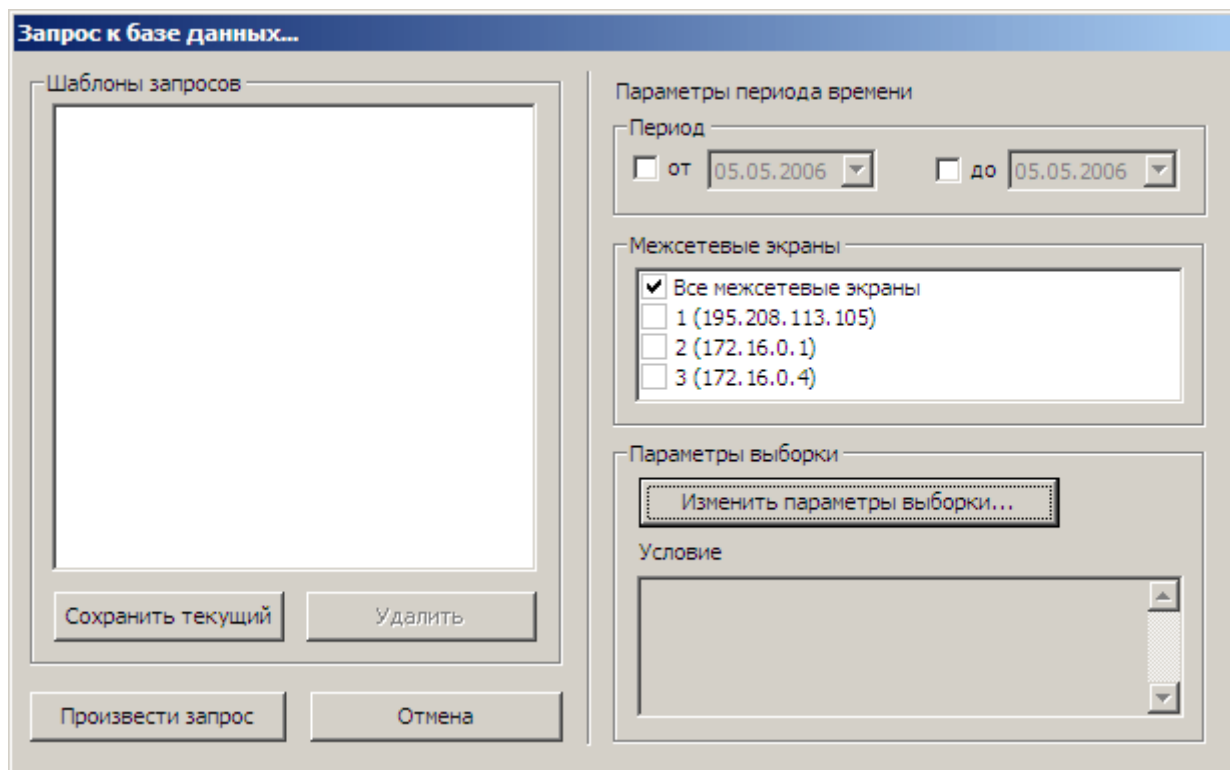


Рис.4.3

Выбор команды **Изменить параметры выборки** в окне запроса к базе данных позволяет изменить параметры выборки по установленные по умолчанию. Открывается форма (рис.4.4) для изменения условий выборки. В этой форме можно выбрать таблицу, поля и вставить необходимые значения или их сочетания для выборки. При вставке значений следует знать, что значения в текстовые поля необходимо вводить в кавычках, а в числовые - без кавычек. Таблицы имеют следующие поля.

Для всех таблиц.

Текстовые поля: Дата, Время, Действие, Входн. интерфейс/ы, Выходн. интерфейс/ы

Числовые поля: Сетевой экран, Правило.

*Для таблицы **ETH**.*

№ изм.	Подпись	Дата

Текстовые поля: Аппаратный адрес приёмника, Аппаратный адрес источника, Тип/длина фрейма, Примечание.

Для таблицы ARP.

Текстовые поля: Тип аппаратного адреса, Тип протокола, Код операции, MAC адрес источника, IP адрес источника, MAC адрес приёмника, IP адрес приёмника.

Числовые поля: Размер MAC адреса, Размер IP адреса,

Для таблицы IPX.

Текстовые поля: Контрольная сумма, Тип пакета, Сеть назначения, Узел назначения, Сокет назначения, Сеть источника, Узел источника, Сокет источника.

Числовые поля: Длина пакета, Счетчик пройденных мостов,

Одинаковые типы полей для таблиц IP, TCP, UDP, ICMP.

Текстовые поля: Приоритет, Тип сервиса, Резервные биты, Флаги, IP адрес источника, IP адрес приёмника.

Числовые поля: Версия, Длина заголовка, Длина пакета, Идентификация, Смещение фрагмента, Время жизни, Протокол, Контрольная сумма.

Специфичные типы полей таблицы IP.

Текстовое поле: Примечание

Специфичные типы полей таблицы TCP.

Текстовые поля: Резервное поле TCP пакета, Контрольные биты, Контрольная сумма.

Числовые поля: Порт источника, Порт приёмника, Номер последовательности, Номер подтверждения, Смещение данных, Размер окна, Указатель срочности.

Специфичные типы полей таблицы таблицы UDP.

Числовые поля: Порт источника, Порт приёмника, Длина пакета, Контрольная сумма.

Специфичные типы полей таблицы таблицы ICMP.

№ изм.	Подпись	Дата

Текстовые поля: Примечание

Числовые поля: Тип IСMP, Код IСMP, Контрольная сумма.

*Для таблицы **СОБЫТИЯ**.*

Текстовые поля: Дата, Время, Время работы (время работы указывается в формате: дней:часов:минут:секунд), Пользователь, Примечание.

Числовые поля: Тип, Событие, Уточнение.

При создании запросов по таблице **СОБЫТИЯ** в поля тип, событие и уточнение необходимо вводить числовые коды событий.

В межсетевом экране ССПТ-1М реализована регистрация событий, которые происходят в процессе работы. В базе данных хранятся числовые коды событий. Далее представлена расшифровка числовых кодов событий.

Все события разделяются по типу на : "Сообщения ", "Предупреждения" и "Ошибки".

1 - Сообщения

257 - Запуск фильтра

258 - Останов фильтра

259 - Приостанов фильтрации

260 - Возобновление фильтрации

261 - Изменение правил

Уточнения для изменения правил

1 - правила фильтрации по MAC-адресам

2 - правила фильтрации по ARP

3 - правила фильтрации по IP

4 - таблица интервалов времени

5 - правила фильтрации по IPX

262 - Начало регистрации пакетов

263 - Останов регистрации пакетов

264 - Очистка журнальных файлов

№ изм.	Подпись	Дата

- 265 - Перезапуск сервера фильтрации
- 266 - Изменение параметров конфигурации фильтра
- 268 - Вход администратора
- 269 - Выход администратора
- 270 - Добавление нового пользователя
- 271 - Удаление пользователя
- 272 - Изменение пароля
- 273 - Запрос на запуск фильтра
- 274 - Запрос на останов фильтра
- 275 - Запрос на перезапуск фильтра
- 276 - Запрос на изменение параметров конфигурации
- 279 - Изменение регистрации неподдерживаемых протоколов
- 280 - Запрос на останов устройства
- 281 - Останов устройства
- 282 - Запрос на изменение правил
- 283 - Запрос на изменение системного времени
- 284 - Изменение системного времени
- 285 - Запрос на очистку журнальных правил
- 286 - Запрос к модулю управления пользователями
- 287 - Запрос на применение правил сервером фильтрации
- 288 - Применение правил сервером фильтрации
- 289 - Запрос на добавление нового пользователя
- 290 - Запрос на удаление пользователя
- 291 - Запрос на изменение пароля
- 292 - Создание файла правил
- 293 - Выгрузка текстового файла правил
- 294 - Запрос на выгрузку текстового файла правил
- 295 - Загрузка текстового файла правил

№ изм.	Подпись	Дата

- 296 - Откат к сохраненной конфигурации
- 297 - Выгрузка журнальных файлов по NFS
- 298 - Проверка целостности компонентов ПО
- 299 - Выгрузка файлов регистрации по FTP
- 301 - Изменение имен интерфейсов
- 267 - Изменение состояния управляющего Ethernet
- Уточнения для изменения состояния управляющего Ethernet
 - 1 - Интерфейс вкл.
 - 0 - Интерфейс выкл.
 - 2 - Статус не изменился
- 277 - Изменение шлюза по умолчанию
- Уточнения для изменения шлюза по умолчанию
 - 1 - Интерфейс вкл.
 - 0 - Интерфейс выкл.
 - 2 - Статус не изменился
- 300 - Изменение параметров выгрузки по FTP

2 - Предупреждения

- 513 - Принят свой собственный Ethernet-кадр
- 514 - Принят неподдерживаемый фильтром Ethernet-кадр
- 515 - Неизвестный тип протокола в IP-пакете
- 516 - Неподдерживаемый протокол внутри кадра Ethernet II
- 517 - Неподдерживаемый протокол внутри кадра IEEE 802.2/LLC
- 518 - Недостаточно привелегий для выполнения операции
- 519 - Пустая маска выходных интерфейсов
- 520 - Отказ в авторизации администратора
- 521 - Отказ в выходе администратора

№ изм.	Подпись	Дата

3 - Ошибки

769 - Ошибка ввода-вывода устройства brf

770 - Ошибка вызовов операционной системы

771 - Ошибка обработки файла конфигурации

772 - Ошибка выгрузки по NFS

Уточнения для ошибки выгрузки по NFS

1 - Ошибка монтирования

2 - Ошибка копирования

773 - Ошибка выгрузки по FTP

Уточнения для ошибки выгрузки по FTP

1 - Ошибка соединения с FTP

2 - Ошибка копирования файла на FTP сервер

На рисунке 4.4 представлен пример параметров запроса: Выбрать из таблицы ETH все кадры типа IEEE 802.3 или кадры, в которых находились пакеты протокола ARP.

Пример параметров запроса

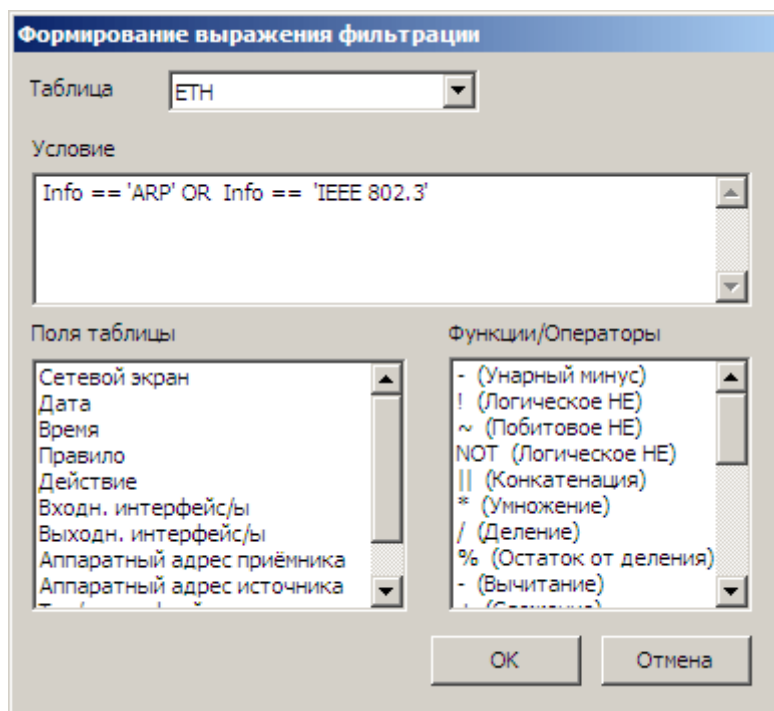


Рис. 4.4

№ изм.	Подпись	Дата

Экспорт - (Ctrl+S) Экспорт данных. Открывается форма (рис.4.5), в которой можно выбрать для экспорта сессии или пакеты.

Окно Экспорт

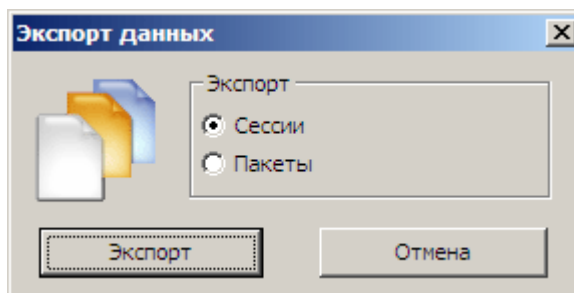


Рис.4.5

Данные можно экспортировать в следующие форматы: Текстовые файлы (*.txt), HTML файлы (*.htm), CSV (XLS) файлы (*.csv), XML файлы (*.xml), RTF файлы (*.rtf).

Параметры страницы - Выбор параметров страницы. Открывается форма, в которой можно выбрать размер бумаги, ориентацию листа и другие параметры.

Предварительный просмотр - Предварительный просмотр документа. Открывается форма, в которой отображается документ перед выводом на принтер.

Печать - (Ctrl+P) Вывод на принтер

Архивировать БД - Архивация базы данных. Сервису конвертации будет отправлена команда архивировать БД. Текущий файл БД будет запакован архиватором и открыт новый файл.

Выход - (Alt+X) Выход из программы

4.2.2. Меню “Вид”

В меню **Вид** (рис.4.6) позволяет включить отображение вертикальной и горизонтальной сетки для сессий и пакетов, а также сменить отображение данных по протоколам.

№ изм.	Подпись	Дата

Меню Вид

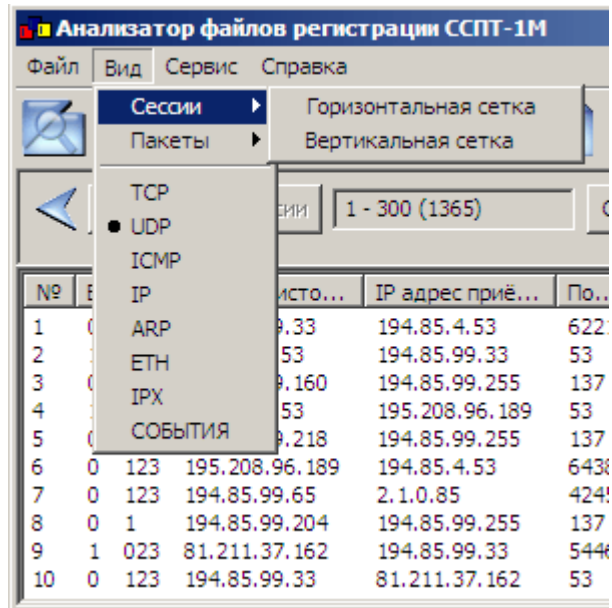


Рис.4.6

4.2.3. Меню “Сервис”

Меню “Сервис” (рис.4.7) предоставляет возможность настройки сервиса конвертации и установки параметров подсистемы визуализации.

Меню “Сервис”

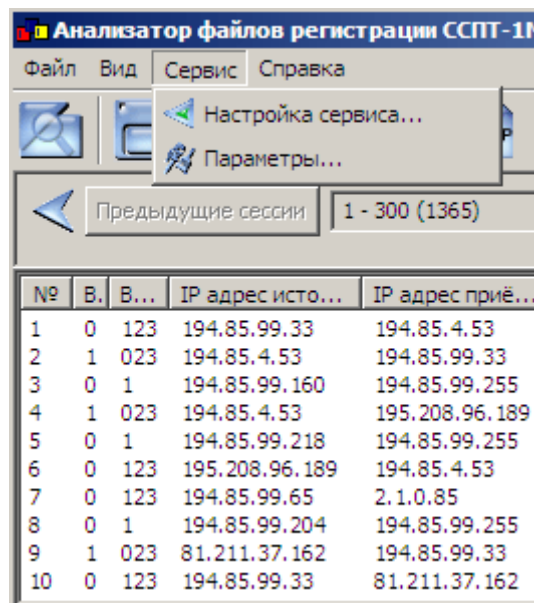


Рис. 4.7

№ изм.	Подпись	Дата

Выбор строки *Настройка сервиса* открывает окно (рис.4.8) настройки и управления сервисом конвертации –**Сервис конвертации**, в котором осуществляется ввод необходимых параметров и управление (старт/стоп) сервисом.

Окно Сервис конвертации

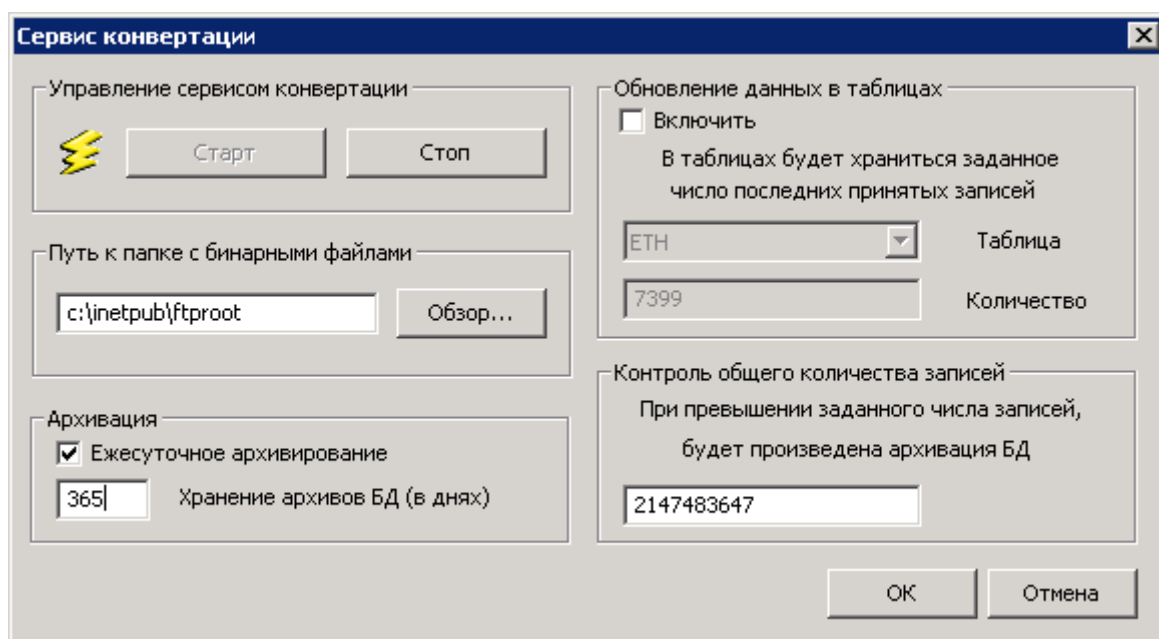


Рис.4.8

Управление сервисом конвертации.

Сервис управляется при помощи кнопок "**Старт**" и "**Стоп**". Если в данный момент сервис работает, то кнопка "**Старт**" не активна, и наоборот - если сервис остановлен, то кнопка "**Стоп**" не активна. После установки программы, перед приемом бинарных файлов, сервис необходимо запустить, в дальнейшем этого делать не нужно, сервис будет запускаться автоматически при старте операционной системы.

Также сервисом можно управлять из меню управления службами Windows: "**Пуск**" - "**Настройка**" - "**Панель Управления**" - "**Администрирование**" - "**Службы**".

Имя сервиса конвертации - **FNPService**.

№ изм.	Подпись	Дата

Путь к папке с бинарными файлами (рис.4.9) должен совпадать с домашним каталогом, который был введен при настройке FTP сервера.

Путь к папке с бинарными файлами

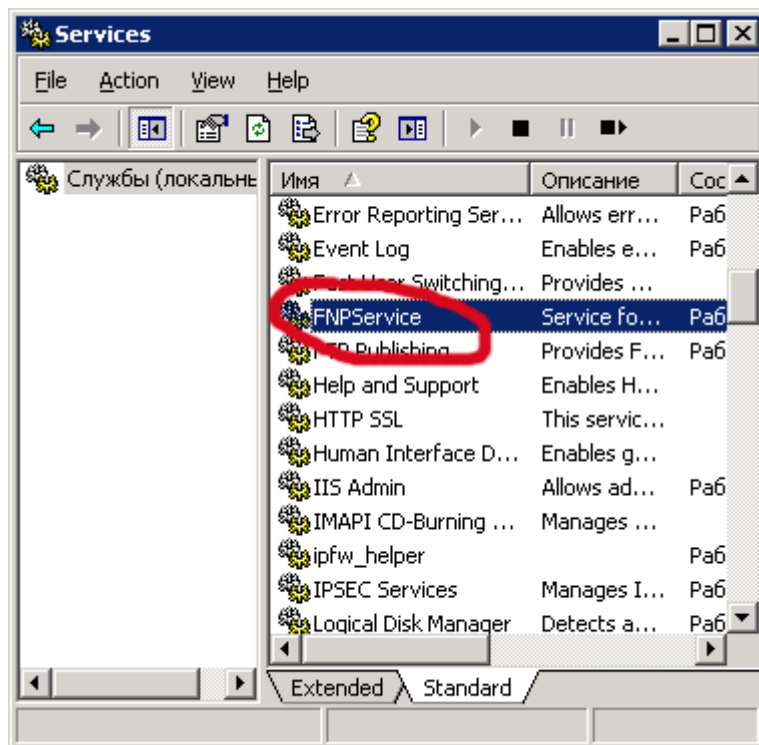


Рис.4.9

Архивация.

В данной секции можно включить ежесуточное архивирование и задать в днях период времени хранения архивов. Создание архивов и контроль периода хранения осуществляется каждый день в 00:00.

Обновление данных в таблицах.

В данной секции можно включить механизм обновления данных в таблицах. Включение этого механизма означает, что в каждой таблице всегда будет содержаться заданное количество записей. Новые поступающие данные будут записываться, а старые удаляться. Таким образом будет осуществляться "вращение" базы данных.

№ изм.	Подпись	Дата

Контроль общего количества записей.

При накоплении заданного общего количества записей, будет произведена архивация БД и открыт новый файл.

При выборе строки *Параметры* меню **Сервис** открывается окно (рис.4.10) для установки параметров подсистемы визуализации.

На странице Директории необходимо указать путь до базы данных. Файл базы данных - ...\\DB\\traffic.db. Если вы не будете сохранять шаблоны запросов, то путь до них указывать не обязательно. Если вы укажете путь, то сохраненные шаблоны запросов будут отображаться в форме "Создать запрос к базе данных"- "Шаблоны запросов".

Указание пути до базы данных и к шаблонам запросов

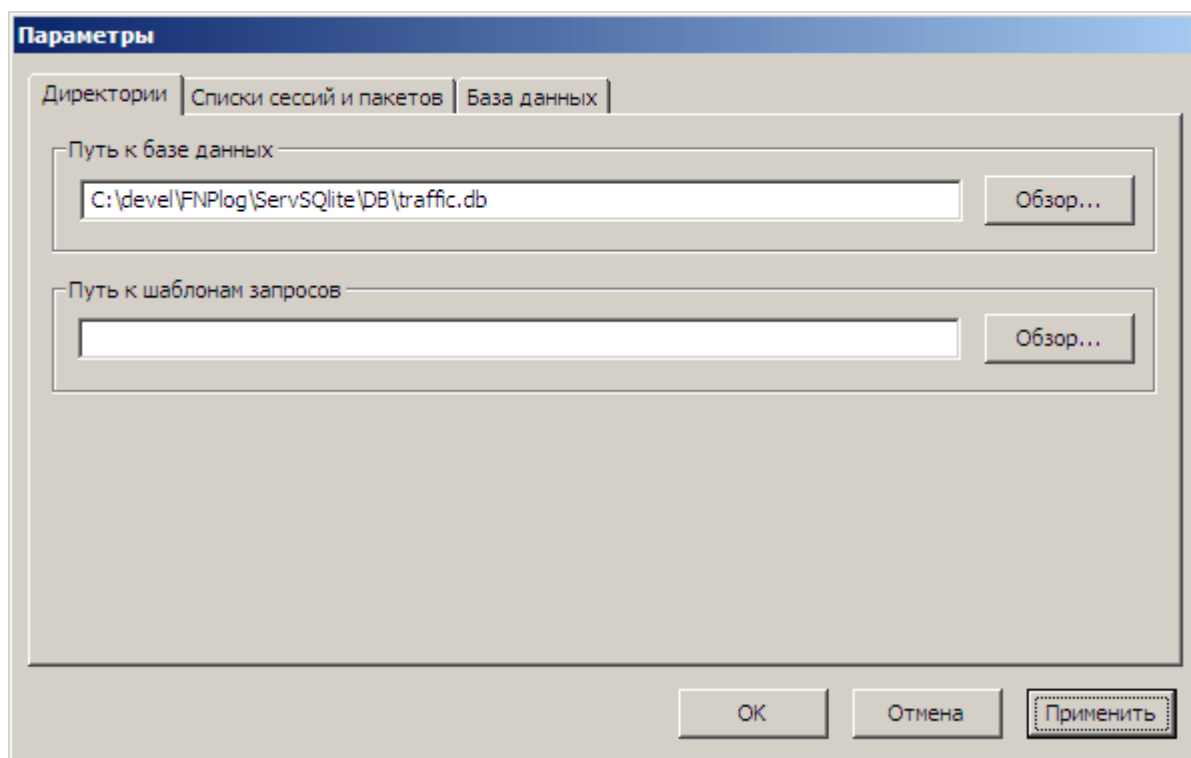


Рис. 4.10

№ изм.	Подпись	Дата

На странице **Списки сессий и пакетов** (рис.4.11) необходимо указать поля, по которым осуществлять суммирование и поля, которые будут отображены при раскрытии сессий.

Страница Списки сессий и пакетов

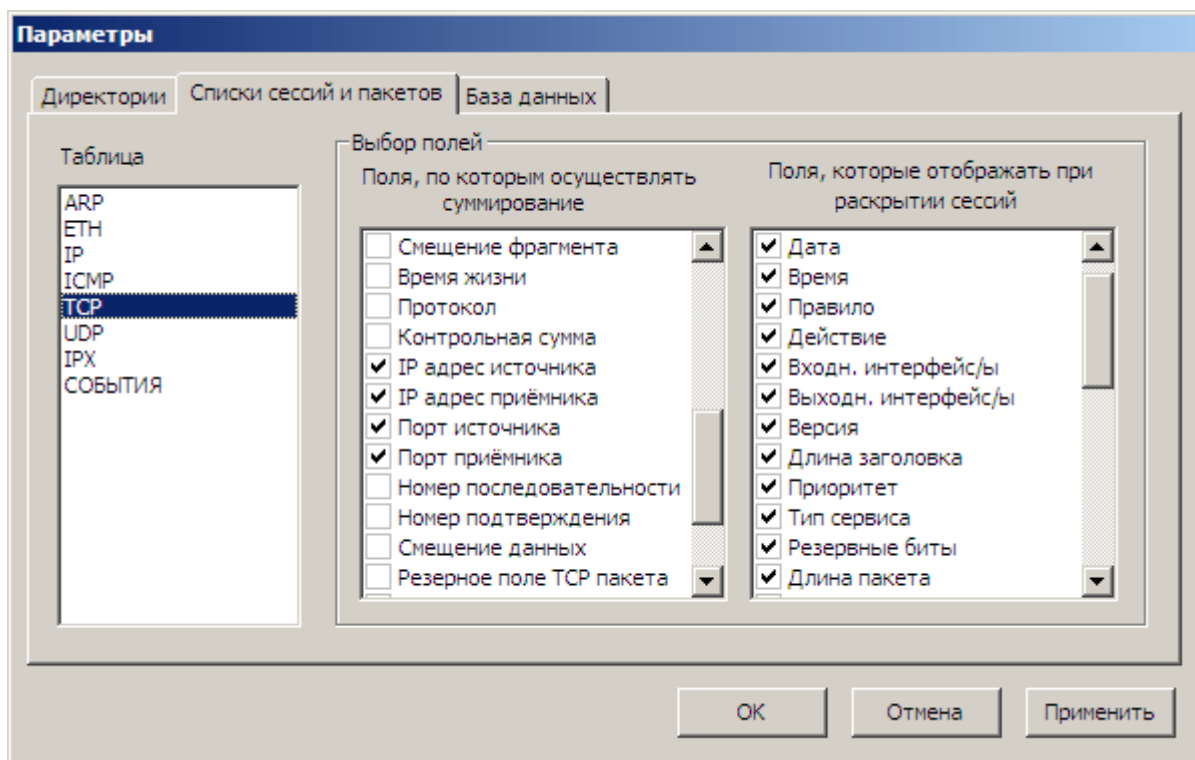


Рис.4.11

Рекомендуются следующие поля суммирования для таблиц:

ARP - "Код операции", "MAC адрес источника", "IP адрес источника".

ETH - "Аппаратный адрес приёмника", "Аппаратный адрес источника", "Примечание".

IP - "IP адрес источника", "IP адрес приёмника", "Примечание".

ICMP - "IP адрес источника", "IP адрес приёмника", "Тип ICMP", "Код ICMP", "Примечание".

TCP - "IP адрес источника", "IP адрес приёмника", "Порт источника", "Порт приёмника".

UDP - "IP адрес источника", "IP адрес приёмника", "Порт источника", "Порт

№ изм.	Подпись	Дата

приёмника".

IPX - "Тип пакета", "Сеть назначения", "Узел назначения", "Сокет назначения", "Сеть источника", "Узел источника", "Сокет источника".

СОБЫТИЯ - "Тип", "Событие".

На странице **База данных** (рис.4.12) необходимо указать количество строк для отображения в списках сессий и пакетов и таймаут для доступа к базе данных. Этот таймаут необходим для того, чтобы обрабатывалась такая ситуация, когда в момент добавления записей осуществляется запрос на выборку.

Страница База данных

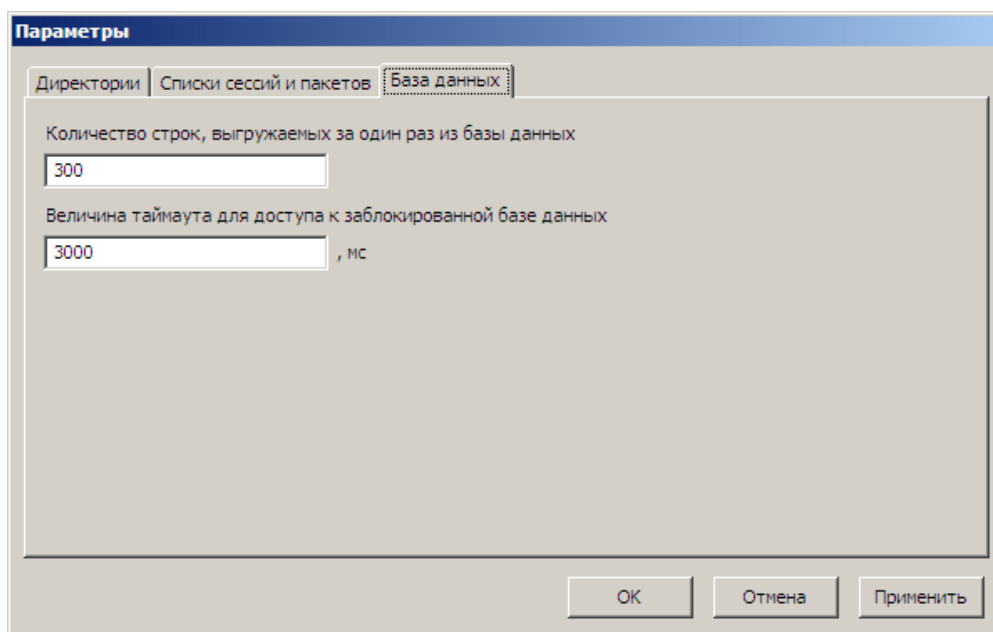


Рис.4.12

4.2.4. Меню “Справка”

Меню “Справка” открывается из главного окна (п.4.1).

Меню “Справка” (рис. 4.13) содержит следующие команды.

“**Вызов справки**” – Вызов оглавления справки о работе с программным комплексом «Анализатор файлов регистрации ССПТ-1М» (F1).

№ изм.	Подпись	Дата

“О программе” – Вывод диалогового окна с информацией о программном комплексе «Анализатор файлов регистрации ССПТ-1М».

Меню “Справка”

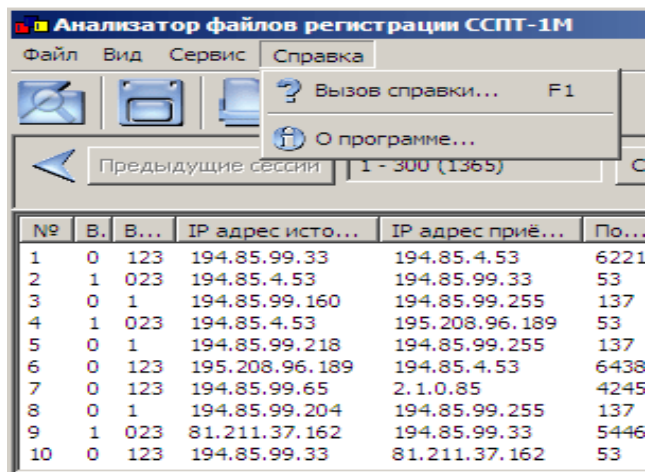


Рис. 4.14

4.3. Параметры построения диаграммы

Окно **Параметры построения диаграммы** (рис.4.15) открывается из главного окна (п.4.1). Диаграмма строится по следующему принципу. Временная ось разбивается на заданный квант времени и подсчитывается количество или суммарный размер пакетов попавших в заданный квант по всем или по заданному (ным) протоколу (лам).

Окно установки параметров диаграммы

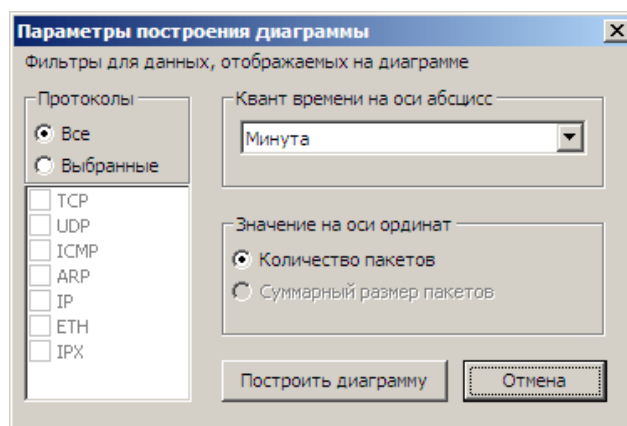


Рис. 4.15

№ изм.	Подпись	Дата

5. ФОРМАТЫ ТАБЛИЦ

Данные, используемые при работе комплекса «Анализатор файлов регистрации ПО ССПТ-1М», хранятся в базе данных, управляемой СУБД SQLite. База данных содержит таблицы с информацией о зарегистрированных пакетах; таблицу с информацией о событиях, происходящих на межсетевых экранах; таблицу со статистической информацией о зарегистрированных пакетах; таблицу с описанием параметров межсетевых экранов, информация от которых хранится в базе данных.

Имена и назначение всех таблиц, содержащихся в базе данных, приведены в Таблице 1.

Таблица 1 – Имена и содержание таблиц, содержащихся в базе данных

Имя таблицы	Содержимое таблицы
Arp	Информация о пакетах протокола ARP/RARP
Eth	Информация о пакетах протокола Ethernet
Ip	Информация о пакетах протокола IP стека TCP/IP
ip_icmp	Информация о пакетах протокола ICMP стека TCP/IP
ip_tcp	Информация о пакетах протокола TCP стека TCP/IP
ip_udp	Информация о пакетах протокола UDP стека TCP/IP
Ipx	Информация о пакетах протокола IPX стека IPX/SPX
Events	Информация о событиях, происходящих на межсетевых экранах
Fnplist	Информация о параметрах межсетевых экранов, информация от которых помещена в базу данных
sqlite_sequence	Статистическая информация с количеством записей в таблицах, содержащих сведения о пакетах регистрируемых протоколов, и таблице событий

№ изм.	Подпись	Дата

Во всех таблицах, кроме содержащей статистическую информацию, существует ключевое поле N, содержащее уникальный номер записи.

Таблицы базы данных, хранящие сведения о пакетах регистрируемых протоколов, а также таблица событий содержат идентичные по назначению поля:

- Timestamp – таймстамп – время, измеряемое в секундах, истекшее с 0 часов 0 минут 0 секунд 1 января 1970 года;
- Date – дата регистрации пакета или события;
- Time – время регистрации пакета или события.

Все таблицы, хранящие сведения о пакетах протоколов, содержат другие поля, идентичные по назначению:

- Rule – правило, по которому межсетевой экран обработал этот пакет;
- Action – действие, предпринятое экраном при обработке пакета;
- In_if – интерфейс межсетевого экрана, на котором был получен пакет;
- Out_if – интерфейсы межсетевого экрана, на которые был отправлен пакет;
- FNP_ID – идентификатор межсетевого экрана, на который получен пакет.

Таблицы, содержащие информацию о зарегистрированных пакетах протоколов стека TCP/IP, имеют и другие поля, идентичные по назначению – поля пакета протокола IP стека TCP/IP:

- Version – версия протокола IP;
- IHL – длина заголовка пакета;
- Precedence – приоритет пакета;
- DTR – тип приоритетного сервиса;
- Reserved_bits – резервные биты поля «Качество обслуживания»;
- Total_Length – длина пакета полностью;
- Identification – идентификатор пакета;
- Flags – флаги фрагментации пакета;

№ изм.	Подпись	Дата

- Fragment_Offset – Смещение фрагмента относительно начала передаваемой информации;
- TTL – «время жизни» пакета;
- Protocol – протокол транспортного уровня, уровня сессий или приложения;
- Header_Checksum – контрольная сумма заголовка;
- Source_Address – IP-адрес источника;
- Destination_Address – IP-адрес приёмника;
- Info – вспомогательная информация о пакете.

В таблице 2 приведено описание специфичных полей для остальных протоколов.

Таблица 2 – Описание полей таблиц

Таблица	Поле таблицы	Содержимое поля
Arp	Hardware_Type	Тип сети
	Protocol_Type	Тип протокола
	Length_Hardware_Address	Размер MAC-адреса
	Length_Protocol_Address	Размер IP-адреса
	Operation_Code	Код операции
	Source_Hardware_Address	MAC-адрес источника
	Source_Protocol_Address	IP-адрес источника
	Target_Hardware_Address	MAC-адрес приёмника
	Target_Protocol_Address	IP-адрес приёмника

№ изм.	Подпись	Дата

Продолжение таблицы 2

Таблица	Поле таблицы	Содержимое поля
Eth	Destination	Аппаратный адрес приёмника
	Source	Аппаратный адрес источника
	Type_Length	Тип/длина фрейма
	Info	Примечание (аналогично протоколам стека TCP/IP)
ip_icmp	Type	Тип ICMP пакета
	Code	Код ICMP пакета
	Checksum	Контрольная сумма пакета
ip_tcp	Source_Port	Порт источника
	Destination_Port	Порт получателя
	Sequence_Number	Последовательный номер
	Acknowledgment_Number	Номер квитанции
	Data_Offset	Смещение данных
	Reserved	Резервное поле TCP пакета
	Control_Bits	Контрольные биты
	Window	Размер окна
	Checksum	Контрольные биты
	Urgent_Pointer	Признак срочности
ip_udp	Source_Port	Порт источника
	Destination_Port	Порт приёмника
	Length	Длина пакета

№ изм.	Подпись	Дата

Продолжение таблицы 2

Таблица	Поле таблицы	Содержимое поля
Ipx	Checksum	Контрольная сумма (старая – не используется)
	Packet_Length	Длина пакета
	Transport_Control	Управление каналом связи
	Packet_Type	Тип пакета
	Destination_Network, Destination_Node, Destination_Socket	Сеть, узел и сокет приёмника
	Source_Network, Source_Node, Source_Socket	Сеть, узел и сокет источника
Events	Uptime	Время работы межсетевого экрана
	Type	Тип
	Event	Событие
	Definition	Описание
	User	Пользователь
	Info	Примечание
Fnplist	IP_address	IP-адрес интерфейса межсетевого экрана
sqlite_sequence	Name	Название таблицы
	Seq	Количество хранящихся в указанной базе записей.

№ изм.	Подпись	Дата

6. К СВЕДЕНИЮ АДМИНИСТРАТОРОВ

ЗАО «НПО РТК» готово ответить на все вопросы, связанные с эксплуатацией нашей продукции. Ваши замечания и предложения, а также сведения о работе программного комплекса «Анализатор файлов регистрации ССПТ-1М» принимаются по адресу:

194064, Санкт-Петербург, Тихорецкий пр., 21, ЗАО "НПО РТК".

т.: (812) 552-06-60

т/факс: (812) 552-45-12

Е-mail: info@npo-rtc.ru

№ изм.	Подпись	Дата