



# TerminET

Персональный сетевой экран

Руководство пользователя

---



# Содержание

<b>1</b>	<b>ВВЕДЕНИЕ</b>	<b>3</b>
1.1	О ПРОГРАММЕ TERMINET	3
1.2	<i>ОСНОВНЫЕ ВОЗМОЖНОСТИ ПРОГРАММЫ</i>	3
<b>2</b>	<b>СТАРТ ПРОГРАММЫ</b>	<b>4</b>
2.1	ИНСТАЛЛЯЦИЯ TERMINET	4
2.2	НАЧАЛО РАБОТЫ В TERMINET	4
2.2.1	<i>Windows 98/Me</i>	4
2.2.2	<i>Windows NT/2000/XP</i>	4
2.2.3	<i>Режим администратора</i>	4
2.3	ОПИСАНИЕ ИНТЕРФЕЙСА TERMINET	5
<b>3</b>	<b>ПОЛЬЗОВАТЕЛИ И ГРУППЫ. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ И ГРУППАМИ</b>	<b>9</b>
3.1	ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ	9
3.2	СОЗДАНИЕ ГРУПП	9
<b>4</b>	<b>ИЗМЕНЕНИЕ РЕЖИМА</b>	<b>10</b>
<b>5</b>	<b>ПРАВИЛА ДЛЯ ТРАФИКА (ПРАВИЛА ДОСТУПА)</b>	<b>10</b>
5.1	СОЗДАНИЕ ПРАВИЛ	10
<b>6</b>	<b>ЖУРНАЛ РЕГИСТРАЦИИ ТРАФИКА</b>	<b>15</b>
<b>7</b>	<b>НАСТРОЙКА РАСПИСАНИЯ РАБОТЫ ПОЛЬЗОВАТЕЛЯ В ИНТЕРНЕТ</b>	<b>16</b>
7.1	НАСТРОЙКА ЕЖЕДНЕВНОГО РАСПИСАНИЯ	17
7.2	НАСТРОЙКА ЕЖЕНЕДЕЛЬНОГО РАСПИСАНИЯ	18
<b>8</b>	<b>WEB СПИСКИ</b>	<b>19</b>
8.1	ЧЕРНЫЕ СПИСКИ	19
8.2	БЕЛЫЕ СПИСКИ	19
8.3	ГЛОБАЛЬНЫЕ И ЛОКАЛЬНЫЕ СПИСКИ	19
<b>9</b>	<b>НАСТРОЙКА СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК (IDS)</b>	<b>20</b>
9.1	СОБЫТИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК	20
<b>10</b>	<b>ПРОБЛЕМЫ С NETBIOS</b>	<b>21</b>

# 1 Введение

## 1.1 О программе TermiNET

Программа TermiNET – это персональный сетевой экран, предназначенный для защиты компьютера от атак из Интернет. TermiNET может работать в одном из следующих режимов защиты:

**Закрытый режим** по умолчанию блокирует весь трафик к Вашему компьютеру и от него. Администратор может выборочно разрешить, например, доступ только по FTP или доступ по FTP, Telnet и Web. Или, например, для осуществления родительского контроля доступ может быть разрешен только к определенному множеству Web-страниц. Список этих страниц может быть определен специальными правилами или **Белым списком URL**.

**Открытый режим** не налагает никаких начальных условий блокировки трафика. Администратор может выборочно закрыть определенный доступ к приложениям, портам и протоколам - например: блокировать все Telnet и FTP, блокировать все входящие соединения через порт 25, блокировать доступ к определенному набору web-страниц. Список недоступных страниц может быть определен специальными правилами или **Черным списком URL**.

**Бумеранг** этот режим разрешает весь выходящий трафик, но блокирует все входящие соединения, кроме тех, которые иницированы Вашим компьютером. В этом режиме машина может использоваться для Web-browsing, FTP и т.д. как обычно, но защищена от атак из Internet.

Программа TermiNET – идеальное решение проблемы защиты в Интернет пользователей, занимающихся малым и средним бизнесом, и домашних пользователей, которые не имеют достаточных средств для установки больших программ защиты.

## 1.2 Основные возможности программы

Основные возможности программы TermiNET включают в себя:

- Создание правил блокирования/разрешения трафика: можно **включить\выключить** те или иные правила.
- Черный список/Белый список – эта особенность обеспечивает возможность запрещать доступ к нежелательным сайтам или разрешать его только к известным желаемым сайтам.
- Встроенная в программу система обнаружения атак (Intrusion Detection System, IDS) позволяет обнаружить и предотвратить действия злоумышленника ("хакера" либо "взломщика"), которые могут привести к проникновению внутрь вашей операционной системы (ОС), либо совершению по отношению к ней каких-либо злоупотреблений.
- Гибкое управление доступом позволяет с помощью IP-адреса (диапазона IP-адресов), URL, порта и/или протокола определять правила.
- Правила могут работать в указанные пользователем дни.
- Для каждого пользователя TermiNET можно настроить расписание доступа к Интернет.
- Простота использования интерфейса "Windows Explorer" делает настройки TermiNET доступными даже для начинающего пользователя.


## 2 Старт программы

### 2.1 Инсталляция TermiNET

Вставьте диск с программой TermiNET в устройство считывания с лазерного диска на Вашем компьютере. Программа установки должна запускаться автоматически. Если автозапуска не будет, войдите в меню **Start** → **Run** и укажите **D:\setup**, где D – Ваше устройство для CD-дисков. Далее следуйте инструкциям по установке программы.


После завершения инсталляции нужно **обязательно** перезагрузить компьютер.

### 2.2 Начало работы в TermiNET

После перезагрузки в системной области в правом нижнем углу экрана рядом с часами Вы увидите значок TermiNET . По умолчанию TermiNET будет установлен в режим **Жёсткий Бумеранг**. В режиме **Жёсткого Бумеранга** анализ поступающей во время соединения информации производится по большому числу параметров (адрес, протокол, порт). Поэтому атаки на Ваш компьютер практически невозможны, даже с компьютера, с которым Вы соединились. Это означает, что Ваш компьютер является невидимым для пользователей **Интернет** и надежно защищен от атак злоумышленников и «взлома».

Работа программы TermiNET зависит от операционной системы, которая установлена на Вашем компьютере.

#### 2.2.1 Windows 98/Me

При старте системы TermiNET загружается с установленными по умолчанию правилами, определенными Администратором системы. Если профили всех пользователей TermiNET в системе были созданы, то подключиться можно двумя способами: дважды щелкнуть по значку TermiNET  или один раз щелкнуть правой клавишей мыши и выбрать **Подключить**. При любом из этих способов пользователь должен будет для входа в систему ввести свой идентификатор и пароль. Ввод идентификатора и пароля позволит войти в систему данному пользователю.

#### 2.2.2 Windows NT/2000/XP

Пользователи будут автоматически подключены к TermiNET на основе их профилей, созданных в системе, в случае если:

- Администратор в программе должен быть членом группы **Администраторы** в системе.
- Пользователь должен хотя бы один раз войти в систему, чтобы программа начала работать.
- В случае добавления, удаления или изменения профилей пользователей в системе, TermiNET должен быть перезапущен для внесения изменений в список пользователей.
- Пользователь не относится к группе **Гости** в системе.

#### 2.2.3 Режим администратора

Если Вы желаете воспользоваться преимуществом расширенных возможностей TermiNET, таких, как блокировка доступа к определенным сайтам или изменение заданного по умолчанию режима работы, Вы должны назначить пароль Администратора.



Меню **Инструменты** -> **Опции** позволяет настроить многие опции системы (Рисунок 2).

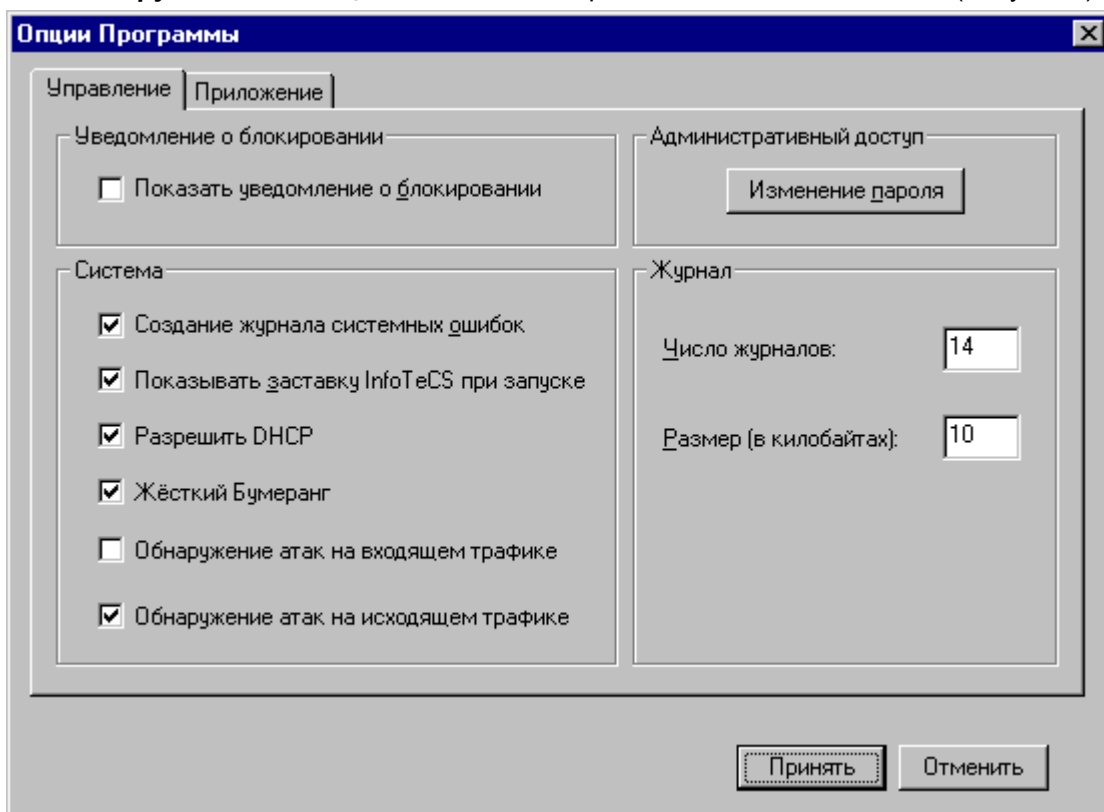


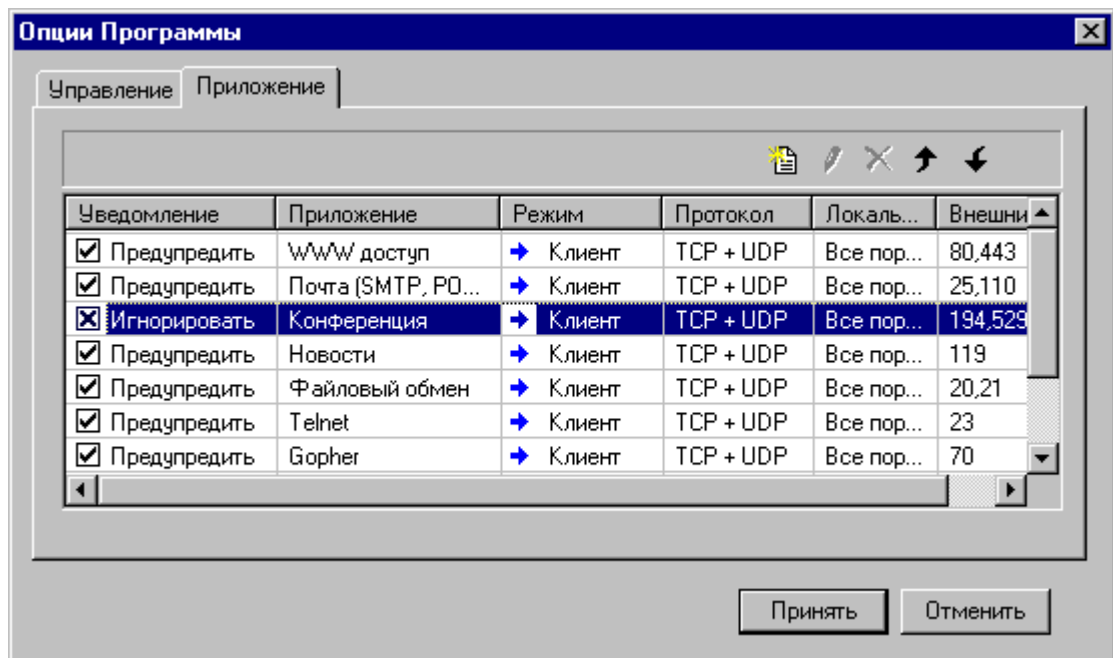
Рисунок 2

Вкладка **Управление** позволяет настроить следующие опции (Рисунок 2):



- **Показать уведомление о блокировании** – при блокировке какого-то пакета на экран выводится окно диалога с уведомлением о блокировании, если эта опция включена. В противном случае это окно не выводится.
- **Создание журнала системных ошибок** – при обнаружении системных ошибок запись о них ведется в файле \Program Files\Infotecs\Terminet\Data\errorlog.txt file.
- **Показать заставку Infotecs при старте программы** – при включении опции при старте программы TerMiNET на экране появится заставка.
- **Разрешить DHCP** – при включении опции программа будет поддерживать протокол динамического распределения IP-адресов (DHCP).
- **Жесткий бумеранг** – по умолчанию опция включена. Если программа установлена в режим **Бумеранг**, то включение этой опции делает режим работы еще более надежным, поскольку в режиме **Жесткого бумеранга** анализ поступающей во время соединения информации производится по большему числу параметров (адрес, протокол, порт). Поэтому атаки на Ваш компьютер практически невозможны, даже с компьютера, с которым Вы соединились. Отключение этой опции устанавливает режим **Мягкий Бумеранг**. В этом режиме анализ поступающей во время соединения информации будет происходить по меньшему числу параметров (адрес и протокол).
- **Обнаружение атак на входящем трафике** – по умолчанию опция выключена. Если ее включить, то программа будет проверять весь входящий трафик Вашего компьютера на сетевые атаки, а при обнаружении атаки - блокировать ее.


- **Обнаружение атак на исходящем трафике** – по умолчанию опция выключена. При ее включении программа будет проверять весь исходящий трафик от Вашего компьютера на сетевые атаки.
- Кнопка **Изменение пароля** – разрешает сменить пароль администратора.
- **Число журналов** – устанавливает число файлов регистрации трафика. При достижении этого числа запись трафика будет вестись в первый файл.
- **Размер (в килобайтах)** – устанавливает размер файла-журнала в килобайтах. При достижении этого размера файл сохраняется, и запись производится в другой файл.

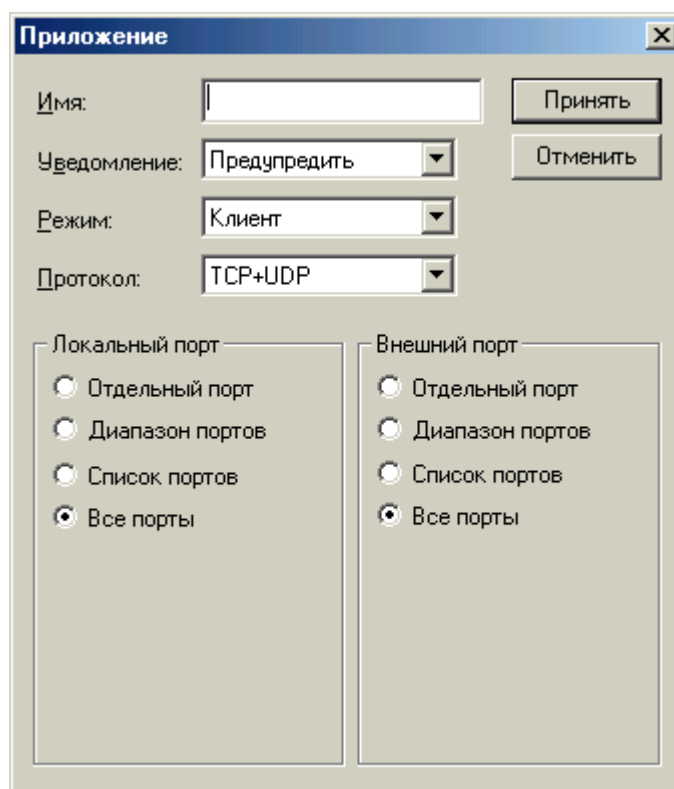
Вкладка **Приложение** (Рисунок 3) содержит стандартные приложения, установленные вместе с программой.



**Рисунок 3**

Данная опция позволяет также создавать новые приложения для настройки правил. Приложения, добавленные пользователем можно редактировать (кнопка ) и удалять (кнопка )

Если щелкнуть мышью на кнопке **Добавить приложение** , то откроется окно **Приложение** (Рисунок 4).



The image shows a dialog box titled "Приложение" (Application). It has a title bar with a close button. The dialog contains the following elements:

- Имя:** A text input field.
- Уведомление:** A dropdown menu with "Предупредить" selected.
- Режим:** A dropdown menu with "Клиент" selected.
- Протокол:** A dropdown menu with "TCP+UDP" selected.
- Локальный порт:** A group box containing four radio buttons: "Отдельный порт", "Диапазон портов", "Список портов", and "Все порты" (which is selected).
- Внешний порт:** A group box containing four radio buttons: "Отдельный порт", "Диапазон портов", "Список портов", and "Все порты" (which is selected).
- Buttons: "Принять" (Accept) and "Отменить" (Cancel) are located on the right side.

**Рисунок 4**

Это окно позволяет настроить следующие опции для добавления нового приложения:

- **Имя** – указать имя приложения.
- **Уведомление** – выбрать *Предупредить* или *Игнорировать* из списка. При выборе *Предупредить* на Вашем экране при блокировке трафика данного типа появится окно с уведомлением о блокировании. При выборе *Игнорировать* окно появляться не будет.
- **Режим** – режим работы Вашего компьютера (*Клиент* или *Сервер*).
- **Протокол** – выбрать протокол из предложенного списка.
- **Локальный порт** – указать настройки порта для локальной машины для этого приложения.
- **Внешний порт** – указать настройки порта для удаленной машины для этого приложения.

После настройки всех опций нужно нажать кнопку **Принять**, после чего новое приложение появится в окне **Опции программы** → вкладка **Приложение** (Рисунок 3). Здесь для каждого приложения (в том числе и для стандартных приложений) вы можете выбрать, требуется ли предупреждение пользователя о блокировке трафика данного типа или нет (колонка **Уведомление**). Для выбора значения щелкните левой кнопкой мыши по пункту в колонке **Уведомление** до появления требуемого значения (*Предупредить* или *Игнорировать*).

### 3 Пользователи и группы. Управление пользователями и группами

Функция добавления пользователей доступна только в случае, если на Вашем компьютере установлена операционная система Windows 98/Me. В Windows NT/2000/XP, пользователь может добавить только группы, которые создаются в организационных целях (см. п. 3.2), а также изменять некоторые свойства пользователя. Для того чтобы изменить свойства пользователя, нужно щелкнуть правой кнопкой мыши на пользователе TermiNET и из появившегося меню выбрать пункт **Пользовательские свойства**. Откроется окно **Свойства пользователя** (Рисунок 5).

#### 3.1 Добавление пользователей

Для того, чтобы добавить пользователя, нужно щелкнуть правой клавишей мыши на самом высоком уровне дерева TermiNET и из появившегося меню выбрать пункт **Добавить пользователя**, или щелкнуть по кнопке **Пользователь** на панели инструментов. Откроется окно **Свойства пользователя** (Рисунок 5).

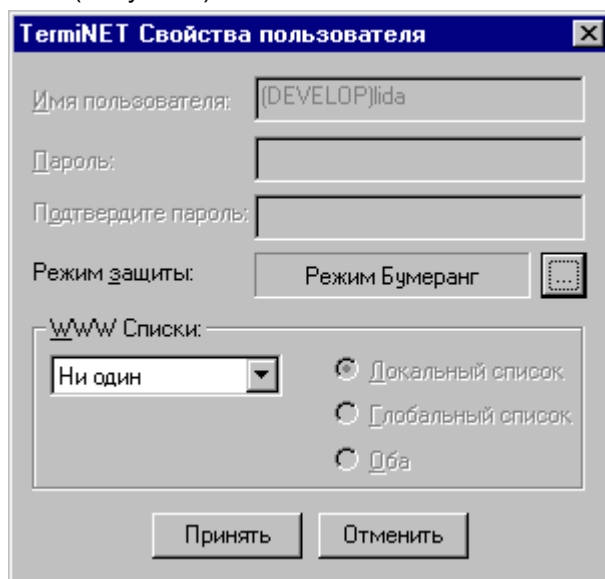


Рисунок 5

Для определения пользовательских свойств нужно заполнить следующие поля:

- **Имя пользователя** – ввести имя желаемого пользователя.
- **Пароль** – ввести пароль для этого пользователя.
- **Подтвердить пароль** – ввести пароль второй раз для подтверждения.
- **Режим защиты** – выбрать режим защиты для установки по умолчанию (п. 1.1).
- **WWW Списки** – определить для этого пользователя использование URL списков (белый, черный, ни один). Справа можно выбрать использование только **локального**, только **глобального** списка или же использовать **оба** списка одновременно.

#### 3.2 Создание групп

Группы используются для организации списков пользователей TermiNET. Для создания новой группы нужно щелкнуть правой клавишей мыши на самом высоком уровне дерева TermiNET и из появившегося меню выбрать пункт **Добавить группу**, затем выбрать по желанию имя для этой группы. Для того чтобы в эту группу добавить пользователя, нужно щелкнуть на

имени этого пользователя и «перетащить» его мышью в создаваемую группу. В этой группе можно и создать пользователя, если щелкнуть мышью на этой группе и выбрать в появившемся меню пункт **Добавить пользователя**.

**Замечание:** Группы пользователей используются только в организационных целях. Специальных настроек правил для групп пользователей не существует.

## 4 Изменение режима

Для изменения режима защиты выберите пользователя, для которого этот режим будет применяться, и в окне **Правила доступа** щелкните мышью по кнопке **Изменение режима**; появится окно **Режим защиты** (Рисунок 6).

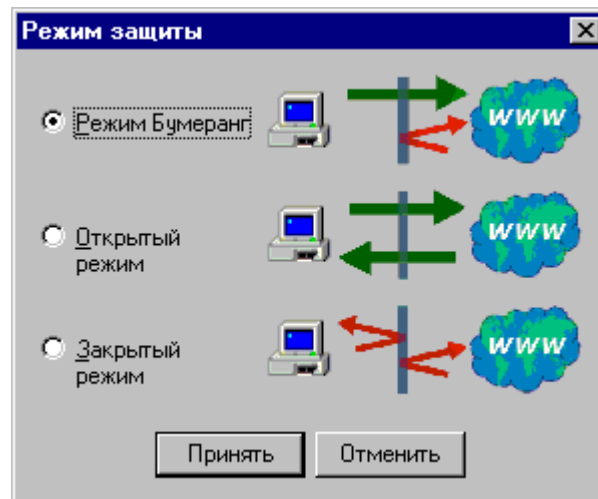


Рисунок 6

Далее установите переключатель в положение требуемого режима и нажмите **Принять**.

Имеется возможность выбрать один из трех режимов работы программы TermiNET. Однако, самый безопасный и удобный режим работы – **Бумеранг**. Режим **Бумеранг** может быть Жёстким и Мягким. Он переключается в меню **Инструменты -> Опции** во вкладке **Управление** (Рисунок 2) – опция **Жесткий Бумеранг**.


Описание режимов защиты вы найдете в п. 1.1.

## 5 Правила для трафика (правила доступа)

Правила для трафика (правила доступа) применяются к определенным IP-адресам или URL и используются для разрешения или запрещения доступа пользователя к некоторым сайтам и сервисам по выбору.

Правила доступа могут определяться во всех режимах работы.

### 5.1 Создание правил

Для того, чтобы добавить новое правило, нужно выбрать конкретного пользователя, к которому это правило будет применяться, и по правой клавише мыши в окне **Правила доступа** из появившегося меню выбрать пункт **Добавить правило** (или щелкнуть мышью по значку  в правом верхнем углу окна **Правила доступа**); появится окно **Введите новое правило** (Рисунок 7).

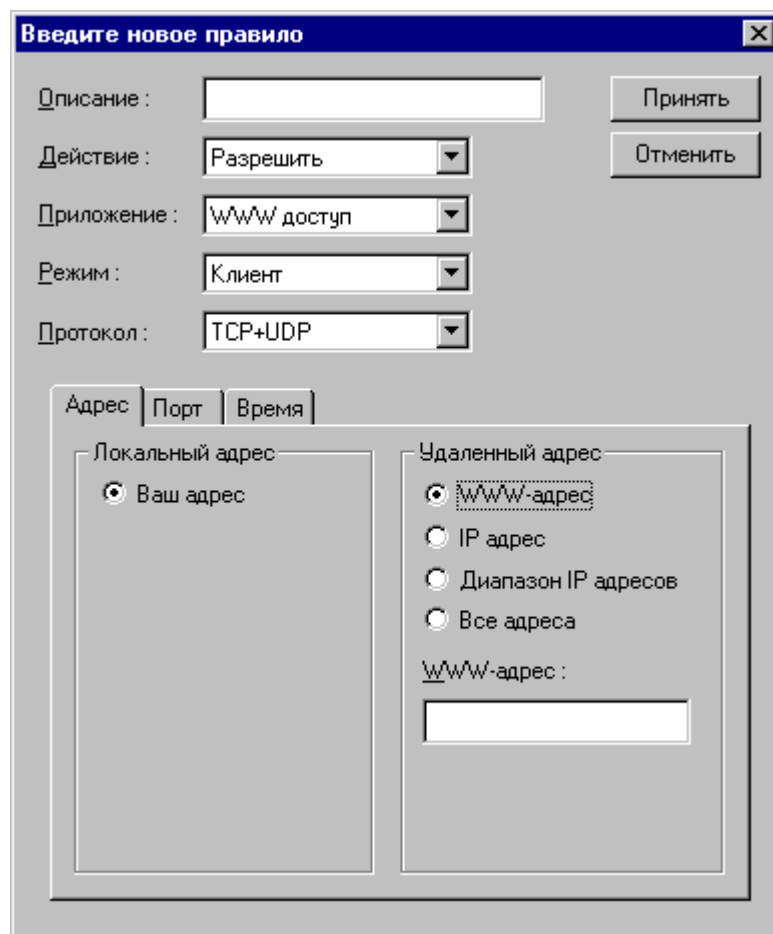


Рисунок 7

Здесь можно настроить следующие опции:

- **Описание** – имя создаваемого правила.
- **Действие** – *Разрешить*, *Блокировать* трафик или сделать *Неактивным* данное правило.
- **Приложение** – приложение можно выбрать из предлагаемого списка.
- **Режим** – указать, *клиентом* или *сервером* будет данная локальная машина для этого правила. *Клиент* означает, что правило применимо для исходящего трафика. *Сервер* означает, что правило применимо для входящего трафика.
- **Протокол** – возможность выбрать протокол для правила.

При выборе приложения в полях **Режим** и **Протокол** появятся определенные для этого приложения значения.

Вкладки **Адрес** (Рисунок 8), **Порт** (Рисунок 9) и **Время** (Рисунок 10) используются для указания дополнительных функций этого правила.

## Адрес

Вкладка **Адрес** определяет в разделе **Локальный адрес** – адрес Вашего компьютера.

Введите новое правило

Описание :

Действие : Разрешить

Приложение : WWW доступ

Режим : Клиент

Протокол : TCP+UDP

Адрес | Порт | Время

Локальный адрес

Ваш адрес

Удаленный адрес

WWW-адрес

IP адрес

Диапазон IP адресов

Все адреса

Введите диапазон IP

Рисунок 8

В разделе **Удаленный адрес** нужно определить URL сайта, IP-адрес или диапазон адресов, к которым применяется правило:

- Выбор опции **WWW-адрес** позволяет ввести этот адрес в поле **WWW-адрес**.
- Выбор опции **IP-адрес** позволяет ввести этот адрес в поле **IP-адрес**.
- Выбор опции **Диапазон IP-адресов** позволяет ввести диапазон адресов (начальный и конечный IP-адрес) в поля **Введите диапазон IP-адресов**.
- Выбор опции **Все адреса** определяет, что правило будет применяться для всех адресов.

## Порт

Вкладка **Порт** используется для указания порта или диапазона портов для правила (Рисунок 9). Эти настройки должны быть сделаны как для локальных, так и для удаленных машин.

Введите новое правило

Описание :

Действие :

Приложение :

Режим :

Протокол :

Адрес | **Порт** | Время

Локальный порт

- Отдельный порт
- Диапазон портов
- Список портов
- Все порты

Внешний порт

- Отдельный порт
- Диапазон портов
- Список портов
- Все порты

Список портов:

80  
443

Добавить | Удалить

**Рисунок 9**

Для локального и внешнего портов можно определить следующие параметры:

- **Отдельный порт** – указать номер отдельного порта для правила.
- **Диапазон портов** – указать диапазон портов для правила.
- **Список портов** – указать список портов для правила.
- **Все порты** – правило будет применимо ко всем портам.

В зависимости от выбранного параметра, в поле ниже этих параметров можно определить конкретные значения данного параметра.

### Время

Вкладка **Время** позволяет настроить выполнение правила в указанные дни недели (Рисунок 10).

Введите новое правило

Описание :

Действие : Разрешить

Приложение : WWW доступ

Режим : Клиент

Протокол : TCP+UDP

Принять

Отменить

Адрес | Порт | **Время**

Временной интервал

<input checked="" type="checkbox"/> Понедельник	Включено
<input checked="" type="checkbox"/> Вторник	Включено
<input checked="" type="checkbox"/> Среда	Включено
<input checked="" type="checkbox"/> Четверг	Включено
<input checked="" type="checkbox"/> Пятница	Включено
<input checked="" type="checkbox"/> Суббота	Включено
<input checked="" type="checkbox"/> Воскресенье	Включено

Рисунок 10

## 6 Журнал регистрации трафика

Для каждого конкретного пользователя в программе ведется *Журнал трафика* (Рисунок 11), где регистрируется и выводится подробная информация о заблокированном и пропущенном IP-трафике, проходящем через компьютер пользователя.

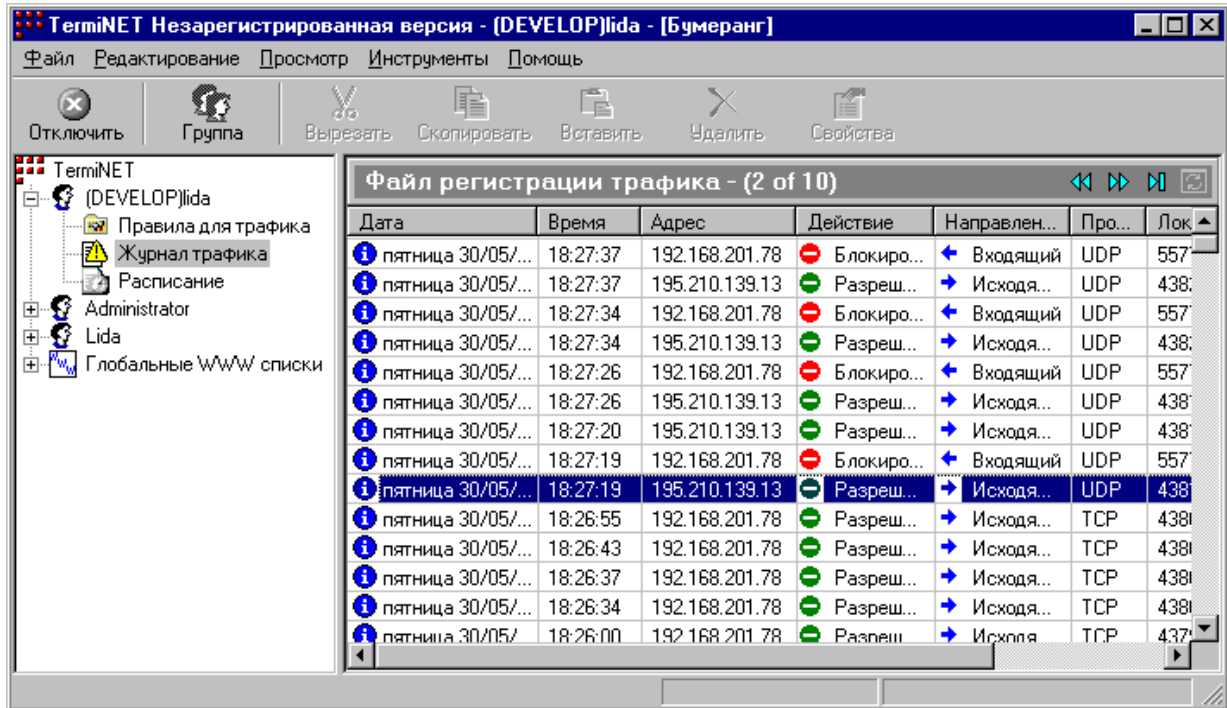


Рисунок 11

Число журналов определяется в меню *Инструменты* -> *Опции* -> *Управление* (Рисунок 2) в разделе *Журнал*. С помощью кнопок (⏪, ⏩, ↺) в правом верхнем углу журнала можно просматривать различные журналы (предыдущий, следующий, вернуться к текущему журналу).

С помощью кнопки (🔄) можно обновить текущий журнал.

## 7 Настройка расписания работы пользователя в Интернет

Для каждого пользователя TermiNET имеется возможность настроить расписание работы этого пользователя в Интернет, т.е. время, когда пользователь сможет или не сможет получать доступ к Интернет.

Для настройки расписания нужно выбрать пользователя, для которого это расписание будет применяться, и щелкнуть левой кнопкой мыши на папке **Расписание** для этого пользователя. В правой части отобразится содержимое окна **Расписание** (Рисунок 12).

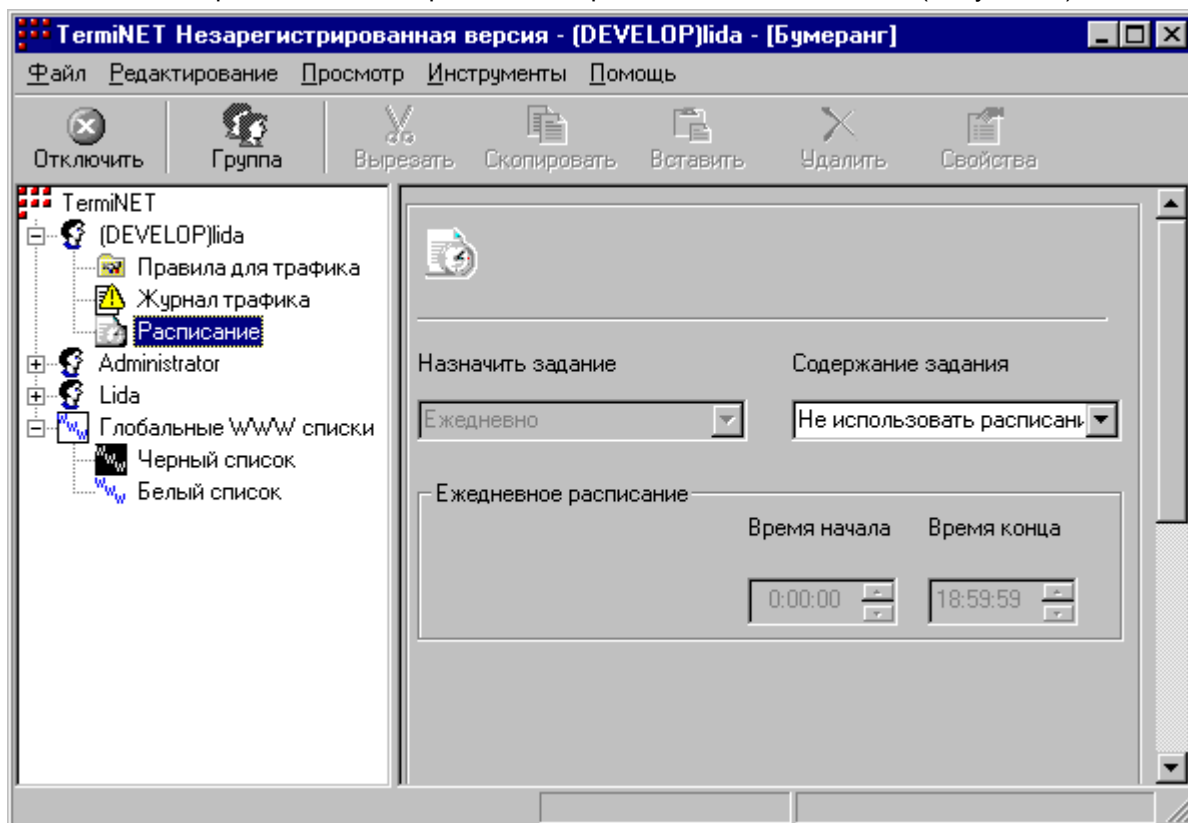




Рисунок 12

Можно настроить следующие опции:

- **Содержание задания** – в выпадающем списке можно выбрать:
  - \* **Не использовать расписание** – означает, что расписание не используется и время, настроенное в расписании ранее, не учитывается (это значение установлено по умолчанию).
  - \* **Разрешить доступ в Интернет** – означает, что пользователь будет иметь доступ в Интернет в заданное в расписании время согласно настройкам режимов и правил, в остальное время доступ в Интернет будет полностью закрыт.
  - \* **Запретить доступ в Интернет** – означает, что пользователь не будет иметь доступа в Интернет в заданное в расписании время, в остальное время доступ в Интернет будет согласно настройкам режимов и правил.

• **Назначить задание** – опция будет доступна для настройки, если выбрано любое значение опции **Содержание задания**, кроме значения **Не использовать расписание**. В выпадающем списке можно выбрать:

- \* **Ежедневно** – возможность настроить ежедневное расписание (см. п.7.1, стр.17);
- \* **Еженедельно** – возможность настроить еженедельное расписание (см. п.7.2, стр.18).

После настройки расписания, в общем списке пользователей в левой части главного окна напротив данного пользователя вместо значка  появится значок наличия расписания -  (Рисунок 13).

### 7.1 Настройка ежедневного расписания

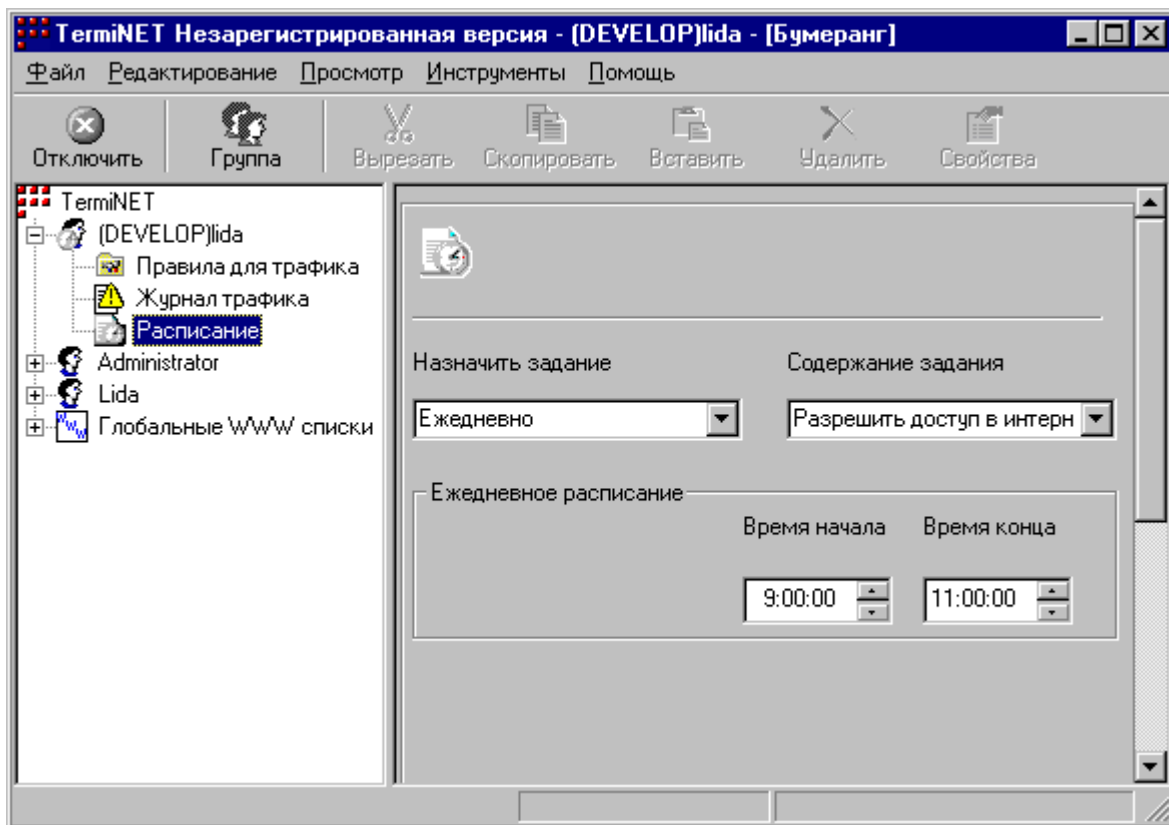


Рисунок 13

Для настройки ежедневного расписания (Рисунок 13) выберите в списке **Назначить задание** значение **Ежедневно**, в списке **Содержание задания** – действие, которое Вы хотите иницировать с помощью расписания (**Разрешить доступ в Интернет** или **Запретить доступ в Интернет**).

Далее в разделе **Ежедневное расписание** в поле **Время начала** задайте время начала действия выбранного задания, а в поле **Время конца** – время окончания. По умолчанию в этих полях стоит значение 00:00, что означает, что выбранное задание действует круглосуточно.

Изменения настроек вступают в силу немедленно.

## 7.2 Настройка еженедельного расписания

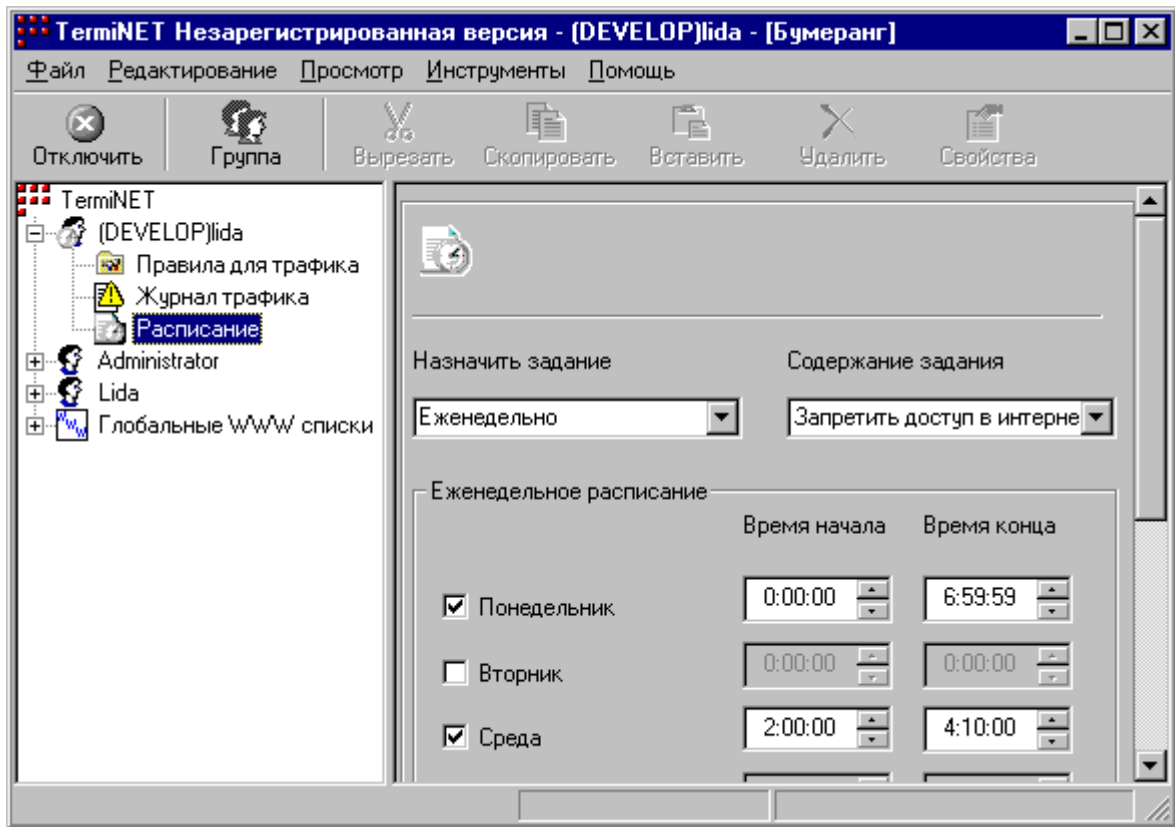


Рисунок 14


Для настройки еженедельного расписания (Рисунок 14) выберите в списке **Назначить задание** значение **Еженедельно**, в списке **Содержание задания** – действие, которое Вы хотите инициировать с помощью расписания (**Разрешить доступ в Интернет** или **Запретить доступ в Интернет**).

Далее в разделе **Еженедельное расписание** задайте для каждого дня недели время начала действия выбранного задания в поле **Время начала** и время окончания в поле **Время конца**. По умолчанию в этих полях стоит значение 00:00, что означает, что выбранное задание действует круглосуточно. Вы можете отключить действие расписания в какой-либо день недели, просто сняв "галочку" напротив этого дня недели (Рисунок 14).

Изменения настроек вступают в силу немедленно.

## 8 Web списки

Web списки могут быть использованы для разрешения и блокировки доступа к определенным сайтам. Списки URL могут быть **Черными** и **Белыми**. **Черные** и **Белые** списки являются взаимоисключающими, то есть для одного пользователя можно определить либо использование **Черного списка**, либо **Белого**.

Для добавления Интернет-сайта в **Черный** или **Белый** список нужно выбрать один из них в левой части интерфейса программы. Далее нажмите на кнопку **Добавить новый адрес**  и появится окно диалога для ввода адресов (Рисунок 15):

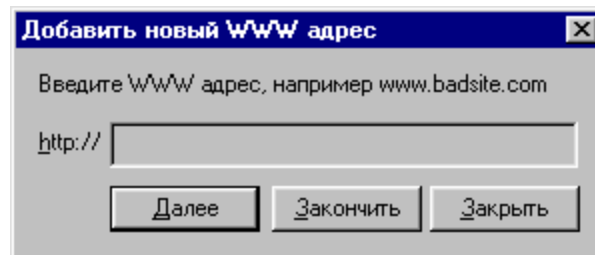


Рисунок 15

В поле ввода этого меню пишется WWW-адрес Интернет-сайта, к которому Вы хотите разрешить/запретить доступ (в зависимости от того, Белый или Черный список Вы выбрали). При нажатии на кнопку **Далее** введенный Вами адрес появляется в списке, а Вы можете ввести еще адрес, и так сколько угодно раз. Для завершения работы в этом окне нужно нажать кнопку **Закончить**. Программа произведет поиск внесенных сайтов и поставит в поле **Существует** значение **Да** – если ресурс будет найден, в противном случае будет стоять значение **Нет**.

WWW-списки можно редактировать и удалять с помощью меню по правой кнопке мыши,

### 8.1 Черные списки

**Черные списки** используются для блокировки доступа к сайтам, к которым правилом доступ разрешен. Например, правило разрешает доступ ко всем Web, а сайт www.notallowed.com внесен в **Черный список**. В связи с этим, пользователю будут доступны все сайты, исключая сайт www.notallowed.com. **Черный список** имеет наибольший смысл назначать для работы пользователя в **Открытом режиме**.

### 8.2 Белые списки

**Белые списки** используются для разрешения доступа к сайтам, к которым правилом доступ запрещен. Например, правило блокирует доступ ко всем Web, а белый список разрешает доступ к сайту www.disney.com, и пользователю не будет доступа ко всем сайтам, исключая сайт www.disney.com. **Белый список** имеет наибольший смысл назначать для работы пользователя в **Закрытом режиме**.

### 8.3 Глобальные и локальные списки

Существует два типа черных и белых списков: **Локальный** и **Глобальный**. Глобальный список создается Администратором и может применяться ко всем пользователям; информация глобального списка будет применяться к тем пользователям, для которых Администратор указал использовать этот глобальный URL список. Локальный список создается только для определенного пользователя, информация из этого списка будет применяться только для пользователя, для которого этот список был создан.

## 9 Настройка системы обнаружения атак (IDS)

Система обнаружения атак работает на сетевом уровне, благодаря чему имеет ряд достоинств:

- Возможность обнаруживать и блокировать сетевые пакеты до обработки их стеком TCP/IP, и этим защищать стек от атак на него самого (такие атаки, как WinNuke).
- Возможность блокировать на ранней стадии атаки, направленные на перезагрузку ОС, приводящие к отказу в обслуживании (например, jolt2 (CAN-2000-0305)).
- Кроме того, IDS способна обнаруживать исходящие атаки (как если бы злоумышленник находился за вашим компьютером). Это полезно в том случае, если ваша ОС каким-либо образом была скомпрометирована (например, с помощью программ – троянских коней) и после используется злоумышленником в качестве атаки на какую-либо третью ОС.

Настройки программы обнаружения атак осуществляются во вкладке **Управление** окна **Опции программы**, открывающегося из меню **Инструменты** -> **Опции**, с помощью включения опций **Обнаружение атак на входящем трафике** и **Обнаружение атак на исходящем трафике** (п. 2.3).

В случае, если программа обнаружит пакет, отвечающий условиям одной из типовых атак, он будет заблокирован. Информация о таких пакетах будет отображаться в журнале.

Описание атак, обнаруживаемых программой IDS, читайте далее.

### 9.1 События системы обнаружения атак

ПО TermiNET обнаруживает следующие виды атак:

#### **Атаки, основанные на особенностях протокола IP**

1001	<b>Атака Land</b>	Попытка злоумышленника замедлить работу вашей машины. Атака использует уязвимость стека TCP/IP, заключающуюся в том, что путем передачи фальшивого TCP-пакета можно заставить атакуемый компьютер попытаться установить соединение самому с собой, путем отправки SYN-пакета с адресом отправителя, идентичным адресу атакуемого компьютера
1002	<b>IP-опции нулевой длины</b>	Попытка злоумышленника вывести из строя ваш внешний сетевой экран путем посылки пакета с IP-опциями нулевой длины
1003	<b>Пустой IP-фрагмент</b>	Обнаружен пустой IP-фрагмент
1020	<b>Атака Jolt2</b>	Обнаружен пакет с некорректным смещением фрагмента, соответствующим атаке Jolt2. Атака заключается в посылке в течение короткого промежутка времени большого числа специально сформированных пакетов с целью замедлить атакуемую систему

#### **Атаки, основанные на особенностях протокола ICMP**

1101	<b>Возможная атака Smurf</b>	Обнаружен ICMP-запрос, отправленный на адрес подсети (х.х.х.0 или х.х.х.255); такой запрос способен инициировать множественные эхо-ответы, которые могут перегрузить сеть или атакуемую систему
1104	<b>ICMP-запрос маски подсети</b>	Обнаружен запрос на получение значения маски подсети. Такая информация может помочь хакеру собрать данные о конфигурации вашей сети
1106	<b>Фрагментация ICMP-</b>	ICMP-заголовок был разбит на несколько фрагментов в

	<b>заголовка</b>	попытке обойти сетевые экраны или системы обнаружения вторжений
--	------------------	---

**Атаки, основанные на особенностях протокола UDP**

1203	<b>Урезанный заголовок UDP-</b>	Обнаружен UDP-пакет с аномально коротким заголовком
1204	<b>Возможная атака Fraggle</b>	Обнаружен UDP-пакет, отправленный на адрес подсети (х.х.х.0 или х.х.х.255) и предназначенный для одного из "отражающих" портов; такой пакет способен инициировать множество ответов, которые могут перегрузить сеть или атакуемую систему
1205	<b>Заикливание портов UDP</b>	Обнаружен UDP-пакет, заикливаемый между двумя "отражающими" портами. Такие пакеты могут отражаться бесконечное число раз, перегружая сеть и ресурсы вовлеченных систем
1206	<b>Атака Snork</b>	Попытка вызова отказа в обслуживании

**Атаки, основанные на особенностях протокола TCP**

1302	<b>Фрагментация TCP-заголовка</b>	TCP-заголовок был разбит на несколько фрагментов в попытке обойти сетевые экраны или системы обнаружения вторжений
1303	<b>Урезанный TCP-заголовок</b>	Обнаружен TCP-пакет с аномально коротким TCP-заголовком
1304	<b>Неправильное смещение Urgent в TCP-заголовке</b>	Множество таких пакетов могут вызвать "зависание" у некоторых реализаций TCP/IP
1305	<b>Атака WinNuke</b>	Попытка привести вашу систему к перезагрузке. Атака использует ошибку реализации стека TCP/IP при отправке пакета Out of Band
1306	<b>TCP-опции нулевой длины</b>	Попытка злоумышленника вывести из строя ваш внешний сетевой экран с помощью отправки пакета с TCP-опциями нулевой длины
1307	<b>Сканирование TCP XMAS</b>	Обнаружен TCP-пакет с установленными битами FIN, URG и PUSH. Злоумышленник пытается определить наличие доступных служб на вашей системе, посылая такие специально сформированные пакеты
1308	<b>Сканирование TCP null</b>	Обнаружен TCP-пакет со сброшенными всеми управляющими битами. Злоумышленник пытается определить наличие доступных служб на вашей системе, посылая такие специально сформированные пакеты

## 10 Проблемы с NetBIOS

При некоторых обстоятельствах у Вас могут возникнуть проблемы при доступе к хостам, использующим NetBIOS по TCP/IP, когда программа находится в режиме **Бумеранг**. Эта проблема возникает, когда ваш компьютер использует широковещательные сообщения для определения IP-адреса какого-либо хоста в сети. В Режиме **Бумеранг** TermiNET блокирует ответные сообщения от хостов, предотвращая тем самым установление соединений. В связи с этим, необходимо отредактировать строки в Вашем хост-файле, связывающий IP-адреса требуемых хостов с их NetBIOS-именами. Хост-файл является простым текстовым файлом, который обычно находится в директории C:\windows для Win'98 или в директории c:\system32\drivers\i т.д. для Win NT и может быть отредактирован с помощью любого текстового редактора. Образец такого файла с именем hosts.sam представлен в примере и поясняет его структуру. Типичный хост-файл выглядит следующим образом:

```
192.168.25.2    myserver.myorg.com
192.168.56.10  nt_server_1
```

Если Вы желаете добавить хост с именем nt\_server\_2 с IP - адресом 192.168.35.23, нужно отредактировать файл следующим образом.

```
192.168.25.2    myserver.myorg.com
192.168.55.10  nt_server_1
192.168.35.23  nt_server_2
```

Эта проблема отсутствует, если в Вашей сети есть сервер WINS.