Инструкция по настройке и эксплуатации программного обеспечения

1. Введение.

1.1. Общие положения.

Программный продукт предназначен для обеспечения защищенных соединений через сеть Интернет, а также, создания изолированных защищенных сегментов в локальных сетях. В соответствии с законодательством Российской Федерации, данный программный продукт может использоваться для защиты технологических каналов связи информационных систем, не относящихся к критической информационной инфраструктуре. В основу решения положен собственный протокол передачи данных, позволяющий проводить криптографические преобразования в сетевых пакетах, не нарушая базовых принципов работы стеков протоколов TCP/IP.

1.2. Состав программного продукта.

Программный продукт состоит из драйвера, программы управления, обеспечивающей работу с базой данных драйвера и программы, отображающей диагностические и статистические данные по интерфейсам и сведения по текущим соединениям.

1.3. Драйвер.

Драйвер программного продукта, разработанный в архитектуре NDIS 5 Intermediate driver и NDIS 6 Filter driver, располагающийся в сетевом стеке драйверов операционной системы Microsoft Windows между драйверами сетевых адаптеров и драйверами протоколов, обеспечивает преобразование или фильтрацию отправляемых и получаемых сетевых пакетов согласно реализованным алгоритмам и примененным настройкам. В соответствии с сетевой семиуровневой моделью OSI (Таблица 1), драйвер, обрабатывая сетевые пакеты (датаграммы), находится на сетевом уровне (L3), что позволяет контролировать весь сетевой трафик между сетевыми адаптерами и стеком протоколов. Учитывая то, что драйвер контролирует и типы пакетов, анализируя Ethernet – заголовки, то можно утверждать, что его функционал распространяется и на канальный уровень(L2). Исходя из того, что драйвер обеспечивает пересчет и корректировку контрольных сумм в заголовках протоколов транспортного уровня, его функциональность обеспечена и на транспортном уровне (L4) модели OSI.

Таблица 1 . Место и задачи драйвера в сетевой модели OSI.

Уровень (Layer)	Наименование уровня OSI (OSI layer description)	Тип данных (PDU)	Первичные задачи драйвера	Действия драйвера при обработке исходящего трафика	Действия драйвера при обработке входящего трафика
L7	Уровень приложений (Application layer)	Данные (Data)	-	-	-
L6	Уровень представления (Presentation layer)		-	-	-
L5	Сеансовый уровень (Session layer)		-	-	-
L4	Транспортный уровень (Transport layer)	Сегменты (Segments)	Анализ заголовков протоколов транспортного уровня (TCP, UDP, …)		Расчет и корректировка контрольных сумм в заголовках протоколов транспортного уровня с расшифрованной полезной нагрузкой
L3	Сетевой уровень (Network layer)	Пакеты (Packets)/ Датаграммы (datagram)	Анализ заголовков протоколов сетевого уровня (IP, ICMP, IGMP, …)	Зашифровывание полезной нагрузки пакетов, пересчет контрольных сумм IP-заголовка / выполнение правил фильтрации на	Расшифровывание полезной нагрузки пакетов, пересчет контрольных сумм IP-заголовка/ выполнение фильтрации незашифрованных пакетов

				незашифрованных пакетах	
L2	Канальный уровень (Data link layer)	Байты (bytes)/ Кадры(frames)	Анализ заголовков протоколов канального уровня (Ethernet 802.3, 802.11, …)	Фильтрация на основе анализа Ethernet - заголовка	Фильтрация на основе анализа Ethernet - заголовка
L1	Физический уровень (Physical layer)	Биты(bits)	-	-	-

Драйвер программного продукта обеспечивает криптографическое преобразование пакетов на основе данных, задаваемых при его настройке. Эти данные расположены в трех таблицах, которые согласно их назначению, называются таблицами хостов(узлов) клиентов, партнеров(туннелей) и серверов. Данные настройки могут быть как общими для всех имеющихся на компьютере-хосте и подсоединяемых позже сетевых интерфейсов, так и отдельными для каждого.

Таблица хостов- клиентов заполняется записями, содержащими уникальный идентификатор соединения ID для подключения клиента к данному серверу и ключевую информацию, на базе которой генерируется криптографический ключ. Для обеспечения соединения на хостах-клиентах должны быть внесены записи в таблице хостов-серверов с указанием, присвоенных каждому клиенту, уникальных идентификаторов соединений, соответствующей клиенту ключевой информацией и, дополнительно, IP-адресом сервера. Соединение устанавливается только по инициативе клиента. Структура записи приведена в Таблице 2 данного описания.

Таблица 2 Структура записи таблицы хостов-клиентов (клиентских локальных сетей).

Название поля записи	Описание
ID	Уникальный идентификатор соединения
IPA	Условный IP-адрес для внутренних задач идентификации при нахождении сервера за сетевым устройством, выполняющим сетевую трансляцию публичных адресов WAN в непубличные адреса локальной сети LAN или DMZ (Destination NAT). Может назначаться автоматически или вручную. Должен быть уникальным среди всех записей трех таблиц. Для клиентов внутренней сети, в этом поле может быть задан IP-адрес локальной сети или подсети с указанием IP-маски в соседнем поле.
IPM	IP-маска сети. Используется, в случае если в поле IPA задан IP-адрес локальной сети или подсети.
KS	Ключевая последовательность байтов, используемая для генерации криптографического ключа соединения.

Таблица хостов-серверов заполняется записями, содержащими идентификатор соединения ID, IP-адрес сервера и ключевую информацию, на базе которой генерируется криптографический ключ. На основе этих данных клиент реализует подключение к серверу передавая в сеть и получая и получая из сети данные в зашифрованном виде, начиная с первого пакета. Уникальными должны быть пары значений – идентификатор соединения ID и IP-адрес. Для реализации соединения, на хосте-сервере должна быть запись в таблице хостов-клиентов с указанием такого же идентификатора соединения и той же ключевой информацией. Структура записи приведена в Таблице 3 данного описания.

Таблица 3 Структура записи таблицы хостов-серверов

Название поля записи	Описание
ID	Уникальный идентификатор соединения

IP	IP-адрес сервера. Если доступ к серверу осуществляется из сети Интернет, то в записи указывается публичный(«белый») адрес.
KS	Ключевая последовательность байтов, используемая для генерации криптографического ключа соединения.

Таблица хостов-партнеров заполняется записями, содержащими идентификатор соединения ID, IP-адрес партнера и ключевую информацию, на базе которой генерируется криптографический ключ. Для реализации соединения, на хосте-партнере должна быть запись в таблице хостов-партнеров с указанием такого же идентификатора соединения и той же ключевой информацией, но IP-адресом противоположной стороны. Соединение устанавливается по инициативе любой из сторон.

Таблица 4 Структура записи таблицы хостов-партнеров (партнерских локальных сетей)

Название поля записи	Описание
ID	Уникальный идентификатор соединения
IP	IP-адрес хоста-партнера или партнерской локальной сети(подсети). Если доступ к хосту-партнеру осуществляется из сети Интернет, то в записи указывается публичный(«белый») адрес.
IPM	IP-маска сети. Используется, в случае если в поле IPA задан IP-адрес локальной сети или подсети.
KS	Ключевая последовательность байтов, используемая для генерации криптографического ключа соединения.

Фильтрацию данных драйвер осуществляет на основе настроек, которые могут быть, как общими, так и индивидуальными для каждого сетевого адаптера. Возможна фильтрация «открытых» пакетов следующих типов: не IP-пакеты, Однонаправленные пакеты (Unicast), Групповые пакеты (Multicast), Широковещательные пакеты (Broadcast), Диагностические (ICMP). При включении фильтрации(отбрасывании) всех этих типов пакетов драйвер переводит компьютер-хост в режим крипто-шлюза.

Все таблицы, входящие в базу данных драйвера, хранятся на диске компьютера-хоста в зашифрованном виде. Ключ шифрования создается в процессе установки программного продукта.

1.4. Программа управления.

Отображает все обрабатываемые драйвером сетевые интерфейсы. Обеспечивает настройку функций фильтрации драйвера, добавление, редактирование и удаление записей в таблицах базы данных драйвера. Взаимодействие программы с драйвером происходит через внутреннюю систему команд. Сохранение данных на жесткий диск и чтение данных с него осуществляет, непосредственно, драйвер. С помощью данной программы можно производить экспорт данных во внешний файл и импорт данных из файла (Сохранение и восстановление конфигурации).

1.5. Программа диагностики и статистики.

Отображает активные «закрытые» соединения. Отображает информацию о принятых и отправленных пакетах по типам и информацию о функциональном наполнении сетевых интерфейсов

1.6. Поддерживаемые операционные системы.

Разработаны, собраны в исполняемые модули, подписаны сертификатами и включены в инсталляционный пакет программные средства для различных, как 32-х разрядных, так и 64-х разрядных, операционных систем Microsoft Windows:

- Для рабочих станций (персональных компьютеров и ноутбуков) - Windows XP/ Vista/7/8/10/11.
- Для серверов – Windows Server 2003/2008/2008R2/2012-2016.

1.7. Межплатформенное взаимодействие.

Разработаны программные средства для операционных систем на базе ядра Linux и MacOS, поддерживающих сетевое взаимодействие по данному протоколу.

2. Настройка.

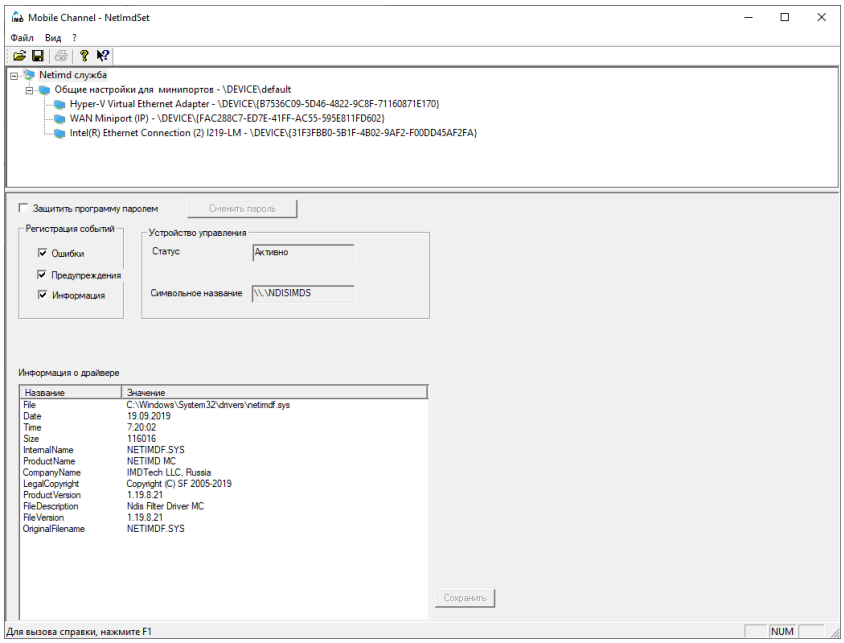
Настройка программного обеспечения производится с помощью программы «NETIMDMC Settings», ярлык которой появляется на «рабочем столе» компьютера в процессе инсталляции. Если при установке программного обеспечения пользователь отказался от создания ярлыков, то найти программу можно по адресу %ProgramFiles%\IMD\NETIMDMC\NetImdSet.exe. Запуск программы настройки требует административных прав. Если программа настройки запущена пользователем без таких прав, потребуется ввести имя и пароль пользователя с административными правами. На этапе установки программного обеспечения производится выбор его режима работы: клиентский или полный(серверный). Программа, установленная для обеспечения серверного режима работы, позволяет производить настройки параметров соединений для трех типов соединений, путем внесения данных в соответствующие таблицы (списки): клиентскую, серверную и партнерскую. Программа, установленная для обеспечения клиентского режима работы, позволяет вносить настройки только в таблицу серверов. Программа отображает информацию о тех сетевых адаптерах, для которых будет производиться преобразование сетевых пакетов в соответствии с настройками для сетевых соединений с заданными в таблице или таблицах данными. Программа позволяет производить, как общие настройки для всех сетевых адаптеров Ethernet, имеющихся в системе (проводных и беспроводных) или для тех которые могут быть подключены позже, так и отдельно для каждого.

Внешний вид программы NetImdSet представлен на Рисунке 1. Программа выполнена в виде стандартного приложения Windows, имеющего меню. Меню обеспечивает выполнение следующих задач:

- Загрузка данных конфигурации драйвера из файла (Файл -> Загрузить);
- Сохранение данных конфигурации драйвера в файл (Файл -> Сохранить, Файл -> Сохранить как);
- Печать текущих данных конфигурации драйвера, просмотр перед печатью, установка настроек принтера (Файл -> Печать, Файл -> Просмотр перед печатью, Файл -> Установки печати);
- Выход из программы (Файл -> Сохранить);
- Отображение/скрытие панели инструментов программы (Вид -> Панель инструментов);
- Отображение/скрытие строки состояния программы (Вид -> Строка состояния);
- Выбор вида отображения данных в таблицах (Вид -> Мелкие значки/Крупные значки/Список/Таблица)

Панель инструментов дублирует функции меню. Строка состояния отображает информацию о состоянии клавиатурных параметров (CapsLock, NumLock).

Ниже расположен элемент управления, имеющий древовидную структуру. При перемещении курсора по элементам изменяется контекст управления, который отображается, непосредственно, под ним. Корневой элемент элемента управления имеет название «Netimd служба». При выборе этого элемента, возможно установить дополнительный пароль на запуск программы. После того, как пароль будет задан, необходимо нажать кнопку «Сохранить».



Кроме того, предоставлена возможность выбрать, события какого уровня важности будут регистрироваться при работе драйвера в системном журнале Windows. Просмотреть события, выбранных на предыдущем этапе типов важности, можно с помощью стандартного приложения Windows «Просмотр событий». Вызов его возможен и из командной строки командами запуска оснасток - *eventvwr.msc* или *compmgmt.msc*.

Рисунок 1 Netimd служба

В таблице «Информация о драйвере» приведены данные о его местоположении в системе, дате сборки, размере, версии, названии продукта и другие.

Для отбора в списке системного журнал только событий, касающихся драйвера данного программного обеспечения следует применить фильтрацию текущего настраиваемого представления по источнику событий: NETIMDF (Рисунок 2).

Настройки для регистрации событий сохраняются в параметре типа REG_DWORD TypesSupported реестра Windows в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\NETIMDF. Источник сообщений для событий, регистрируемых в системном журнале указан в том же разделе в параметре типа расширяемый строковый параметр (REG_EXPAND_SZ) EventMessageFile. По умолчанию, источником сообщений для событий является файл драйвера (netimd.sys или netimdf.sys). Для более информативного наполнения журнала, можно указать в качестве источника сообщений специализированную библиотеку сообщений для событий, предварительно скопировав его из дистрибутива в соответствующий раздел операционной системы: файл %SystemRoot%\System32\netimdfx64.dll для 64-х разрядной ОС или %SystemRoot%\System32\netimdf.dll для 32-х разрядной ОС.

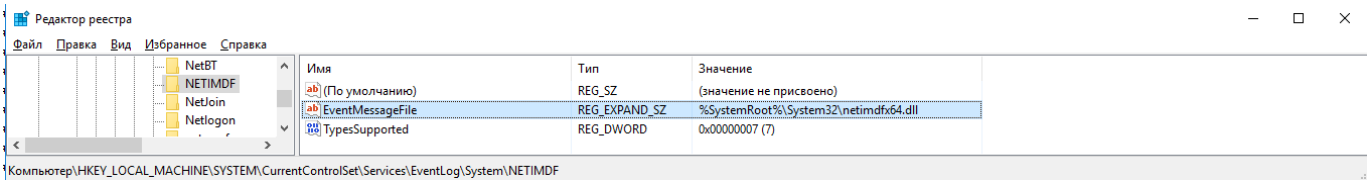


Рисунок 2 Пример настроек реестра Windows для регистрации событий, создаваемых драйвером

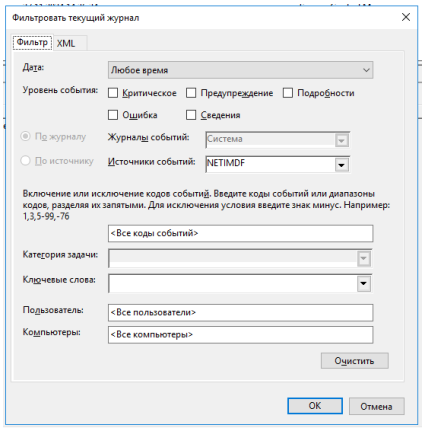


Рисунок 3 Фильтр для системного журнала Window

После применения фильтра можно просмотреть все зарегистрированные события, связанные с работой драйвера программного обеспечения (Рисунок 3).

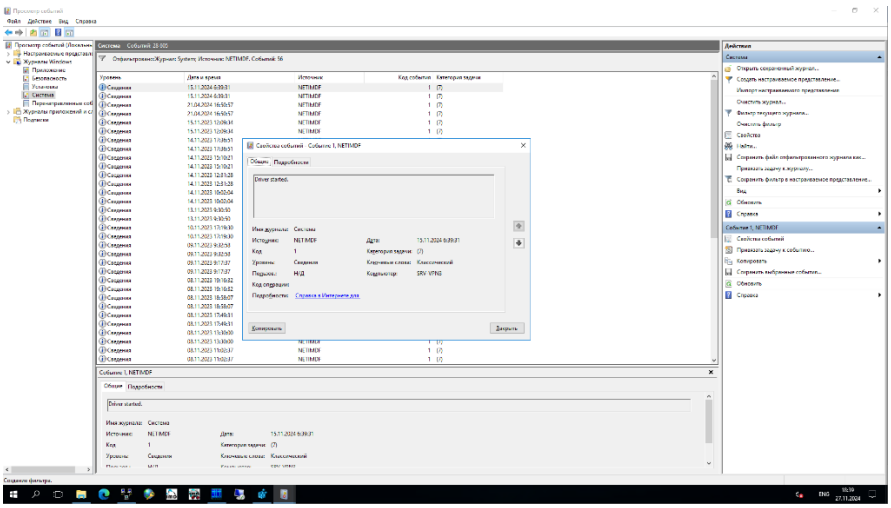


Рисунок 4 События в системном журнале Windows связанные с работой драйвера.

2.1. Настройка программного обеспечения для клиентского режима работы.

Настройка может выполняться как для всех сетевых интерфейсов (в контексте «Общие настройки для минипортов»), так и для каждого сетевого интерфейса отдельно (в контексте конкретного сетевого адаптера). Для сохранения произведенных изменений в настройках, необходимо нажать кнопку «Сохранить», внизу

2.1.1. Настройка параметров преобразования.

Настраиваются два параметра преобразования сетевых Ethernet-пакетов – протокол преобразования (UDP или TCP) и номер порта выбранного протокола. Для подключения через сеть общего пользования рекомендуется выбирать протокол UDP. Выбор номера порта производится исходя из возможности пропуска сетевых пакетов через коммутационное оборудование. Может оказаться, что провайдер не пропускает в Интернет, например, пакеты UDP с указанным портом назначения 80. В таком случае, требуется обратиться в службу поддержки провайдера или подобрать номер порта экспериментально. Разработчик, со своей стороны, планирует выпустить вспомогательную программу для автоматизации процесса подбора номера порта.

2.1.2. Настройка параметров фильтрации.

Программа позволяет провести настройки, обеспечивающие фильтрацию пакетов определенных классов:

- Не относящихся к стеку протокола TCP/IP версии 4;
- Однонаправленных IPv4-пакетов, над которыми не производятся преобразования (Unicast IPv4);
- Групповых (Многоадресных) IPv4-пакетов (Multicast IPv4);
- Широковещательных IPv4-пакетов (Broadcast IPv4);
- Пакетов протокола ICMP стека протоколов TCP/IP версии 4, над которыми не производятся преобразования;

Отдельно задаются правила фильтрации для принимаемых и для оправляемых сетевых пакетов. Правила фильтрации могут быть заданы общие для всех сетевых интерфейсов, так и особые для каждого отдельно.

При отключении возможности приема и передачи по всем указанным классам пакетов, компьютер может взаимодействовать только с узлами(хостами), заданными в таблице серверов. В этом случае следует учесть, что и получение сетевым интерфейсом компьютера IPv4-адреса от DHCP-сервера становится невозможным. Поэтому сетевому интерфейсу с полной фильтрацией «открытых» пакетов должен быть задан статический IPv4-адрес. Следует отметить, что протокол ARP не фильтруется.

2.1.3. Настройка прочих параметров драйвера.

Драйвер снабжен служебной функцией очистки памяти от неиспользуемых данных. К таким данным относится, например, ключ преобразования пакетов для «закрытого» соединения, которое не используется определенное время. Превышение временного интервала, прошедшего с момента последней активности соединения (последнего принятого или переданного пакета), заданного при настройке(по умолчанию – 10 секунд), является сигналом к очистке области оперативной памяти на уровне ядра ОС, занимаемой динамической информацией об этом соединении и ее освобождении. Функция вызывается с периодичностью, задаваемой параметром «Интервал функции периодического таймера».

2.1.4. Работа с таблицей серверов.

Настройка заключается в заполнении таблицы серверов. Предварительно, на аналогичном серверном программном обеспечении заполняется таблица клиентов. Каждому клиенту выделяется уникальный идентификатор и соответствующая ему ключевая информация, на основе которой производится «закрытие» сетевых пакетов, которыми обмениваются по сети Ethernet клиент и сервер. Описание способа получения этой первичной информации, для заполнения таблицы на стороне клиента находится вне рамок данного документа. Таким образом, для реализации подключения к серверу, на клиентском программном обеспечении выполняется операция заполнения записи в таблице серверов аналогичной информацией, за одним исключением: добавляется IPv4-адрес сервера или IPv4-адрес публикации сервера, если тот находится за маршрутизатором, выполняющим преобразование этого адреса в реальный адрес защищаемого интерфейса сервера.

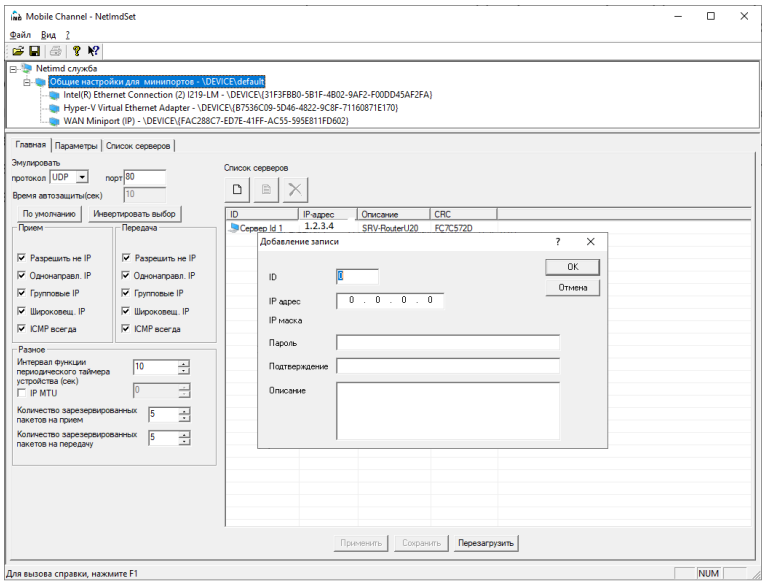


Рисунок 5 Контекст общих настроек

Добавление записи для защищенного соединения с сервером сводится к заполнению полей идентификатора клиента, IPv4-адреса сервера, ключевой информации(пароля) и названия сервера. Если заполнение данных производилось в контексте «Общие настройки минипортов», то для применения на необходимом для соединения сетевом адаптере, необходимо переместить курсор на этот адаптер в списке устройств программы и нажать кнопку «Перезагрузить». Контроль правильности ввода ключевой информации(пароля) может осуществляться сравнением контрольных сумм, отображаемых в поле записи.

Возможно производить индивидуальные настройки для каждого сетевого адаптера. В этом случае, после внесения первой же записи для конкретного адаптера и нажатия кнопки «Перезагрузить», все общие записи для этого адаптера станут недоступны. Чтобы вернуть общие записи, необходимо нажать кнопку «Общие» в контексте этого адаптера.

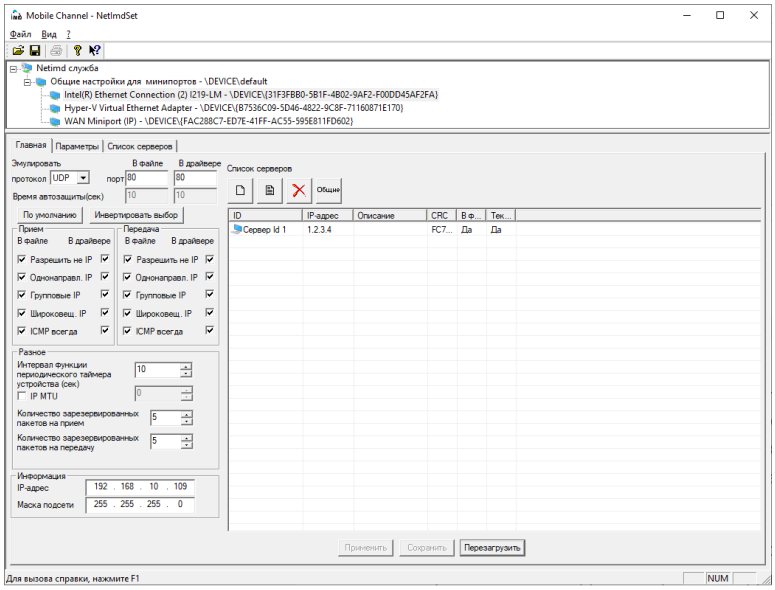


Рисунок 6 Контекст настроек для адаптера

2.2. Настройка программного обеспечения для серверного режима работы.

Данному вопросу посвящен отдельный документ – Руководство Администратора.

2.3. Настройка программного обеспечения для режима работы туннеля.

Данному вопросу посвящен отдельный документ - Руководство Администратора.