1. Введение.

1.1. Общие положения.

Программное обеспечение предназначено для обеспечения защищенных соединений как через сеть Интернет, так и, создания изолированных защищенных сегментов в локальных сетях. В соответствии с законодательством Российской Федерации, данный программное обеспечение 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 стека протоколов TCP/IP.

1.2. Состав программного обеспечения.

Программное обеспечение состоит из драйвера и программы управления, обеспечивающей его настройку. Кроме того, имеется вспомогательная программа, для получения диагностических и статистических данных по интерфейсам и сведений по текущим соединениям.

1.2.1. Драйвер.

Драйвер программного обеспечения для операционных систем Microsoft Windows XP/ Windows Server 2003 выполнен как промежуточный сетевой драйвер (NDIS 5 Intermediate driver). Для последующих версий операционных систем Microsoft Windows - как сетевой фильтр (NDIS 6 Filter driver). Типы драйверов, присутствующие в установочном комплекте, указаны в Таблице 1.

Драйвер использует функции и макросы стандартных библиотек, имеющихся в операционной системе Microsoft Windows:

- NtosKrnl, экспортирующей функции ядра, находящейся в модуле ntoskrnl.exe;
- NDIS, упакованной в Ndis.sys, библиотеки экспорта в режиме ядра.

Таблица 1 Информация о драйверах в установочном комплекте.

Операционная система Microsoft	Архитектура процессора(-ов) компьютера					
	x86-32			x86-64		
	Промежуточный драйвер NDIS 5.X	Фильтр-драйвер NDIS 6.X	Подкаталог инсталлятора	Промежуточный драйвер NDIS 5.X	Фильтр-драйвер NDIS 6.X	Подкаталог инсталлятора
Windows XP/ Windows Server 2003	+	-	i386\WXP	+	-	x64\WXP
Windows Server 2003R2	+	-	i386\WNET	+	-	x64\WNET
Windows Vista (Longhorn)/ Windows Server 2008	+	+	i386\WLH	+	+	x64\WLH
Windows 7/ Windows Server 2008R2	-	+	i386\WIN7	-	+	x64\WIN7
Windows 8/ Windows 8.1/ Windows Server 2012/ Windows Server 2012R2	-	+	i386\WIN8	-	+	x64\WIN8
Windows 10/ Windows Server 2016/ Windows Server 2019	-	+	i386\WIN10	-	+	x64\WIN10
Windows 11/ Windows Server 2022				-	+	x64\WIN10

Располагающийся в сетевом стеке драйверов операционной системы Microsoft Windows между драйверами сетевых адаптеров и драйверами протоколов, драйвер обеспечивает преобразование или фильтрацию отправляемых и получаемых сетевых пакетов согласно реализованным алгоритмам и примененным настройкам. В соответствии с семиуровневой моделью сетевого взаимодействия открытых систем (Open System Interconnection или OSI), отраженной в ГОСТ Р ИСО/МЭК 7498-1-99, 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 содержит информацию о работе, выполняемой драйвером на указанных уровнях модели OSI.

Таблица 2 . 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 незашифрованных пакетах	Расшифровывание полезной нагрузки пакетов, пересчет контрольных сумм IP-заголовка/ выполнение фильтрации незашифрованных пакетов
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 обеспечения 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 3 данного описания.

Таблица 3 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 4 данного описания.

Таблица 4 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 5 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. В этом режиме драйвер пропускает без преобразования только пакеты протокола определения физического адреса устройства (MAC - адреса) по логическому адресу сетевого уровня (IP - адресу) – ARP (Address Resolution Protocol).

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

При установке программного обеспечения, драйвер регистрируется в системе и загружается при включении или перезагрузке компьютера (Start=1 или SERVICE_SYSTEM_START), как драйвер устройства (Type=1 или SERVICE_KERNEL_DRIVER), после инициализации ядра ОС.

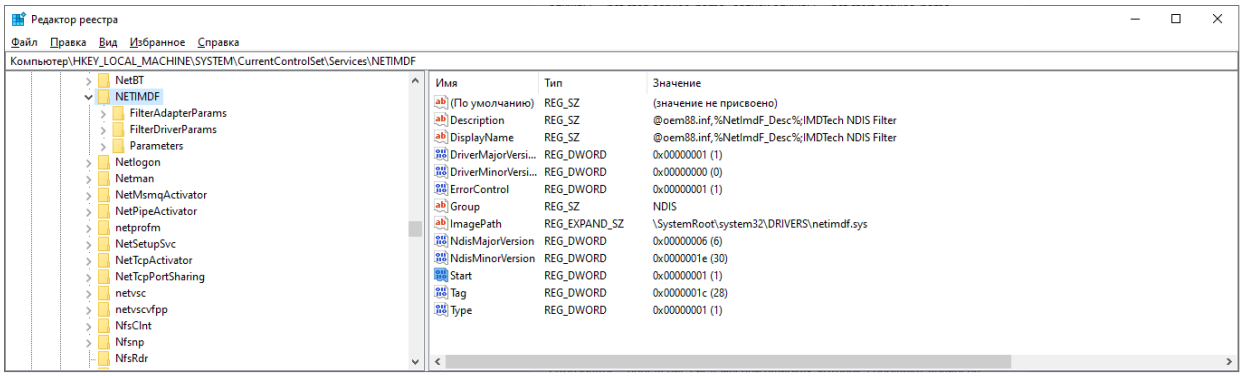

Рисунок 1 Регистрация драйвера в реестре Windows

1.2.2. 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).

1.2.3. Программа диагностики и статистики.

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

1.3. 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.

1.4. Виртуализация.

Возможно использовать данное программное обеспечение на виртуальных машинах с указанными в п. 1.4. операционными системами, под управлением различных гипервизоров. Проверена стабильная работа программного обеспечения на виртуальных машинах под гипервизорами VMWare ESXi версий с 4.0 до 6.7.

1.5. 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*.

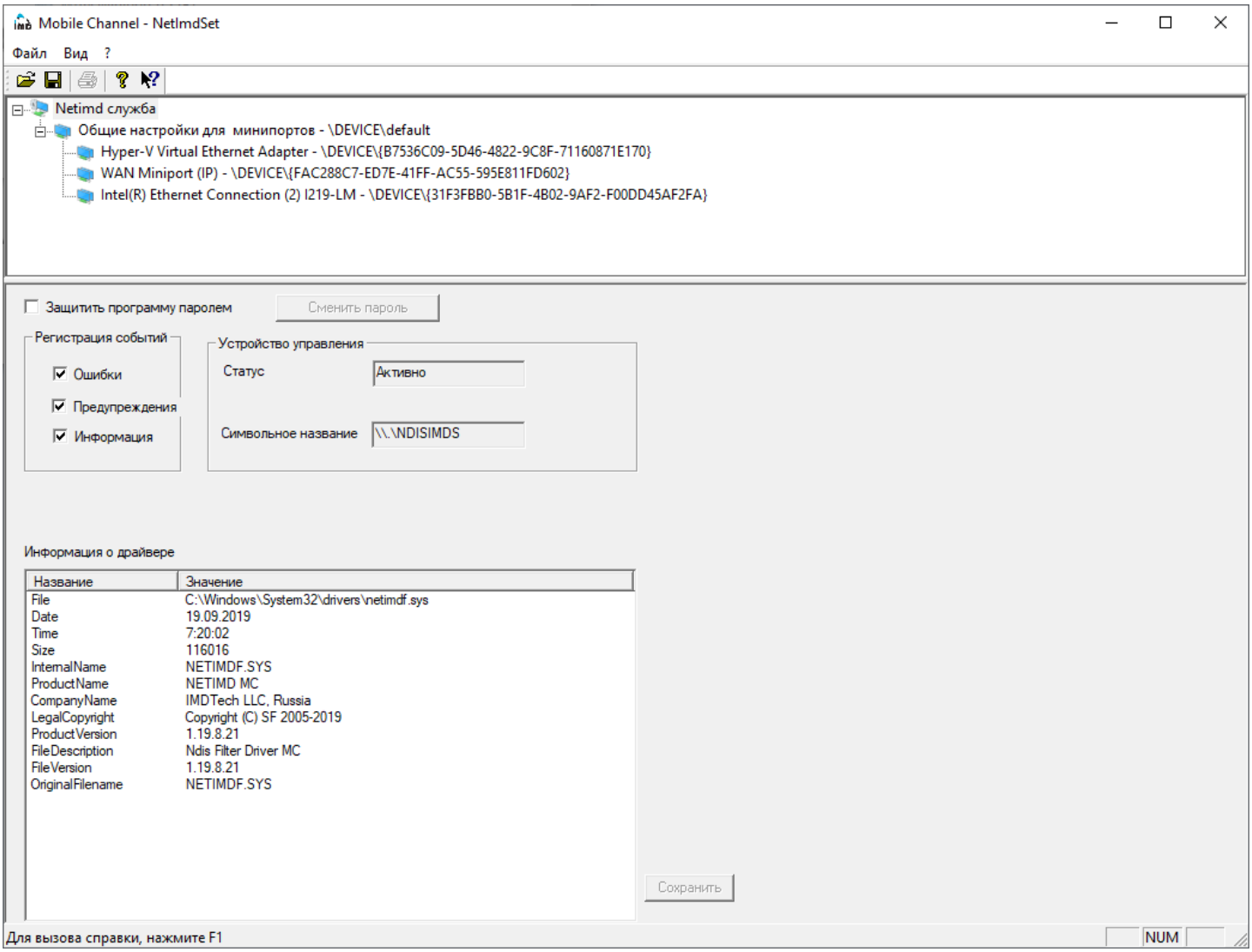

Рисунок 2 NetimdSet – настройки регистрации событий и информация о драйвере.

В таблице «Информация о драйвере» приведены данные о его местоположении в системе, дате сборки, размере, версии, названии программного 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 4).

Настройки для регистрации событий сохраняются в параметре типа REG_DWORD TypesSupported реестра Windows в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\NETIMDF (Рисунок 3). 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.

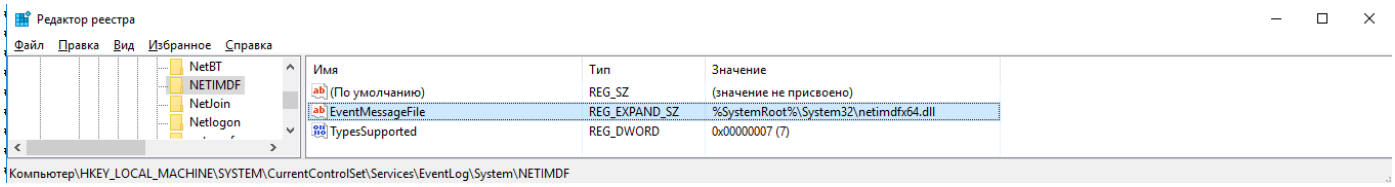

Рисунок 3 Пример настроек реестра Windows для регистрации событий, создаваемых драйвером

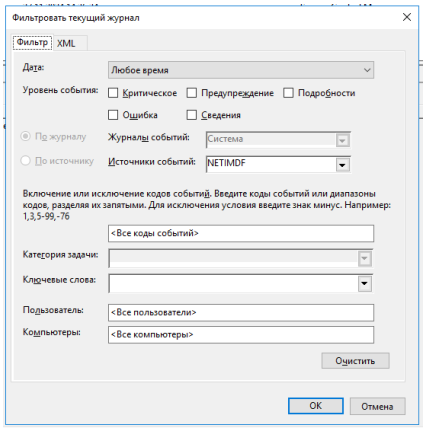

Рисунок 4 Фильтр для системного журнала Window

После применения фильтра можно просмотреть все зарегистрированные события, связанные с работой драйвера программного обеспечения (Рисунок 5).

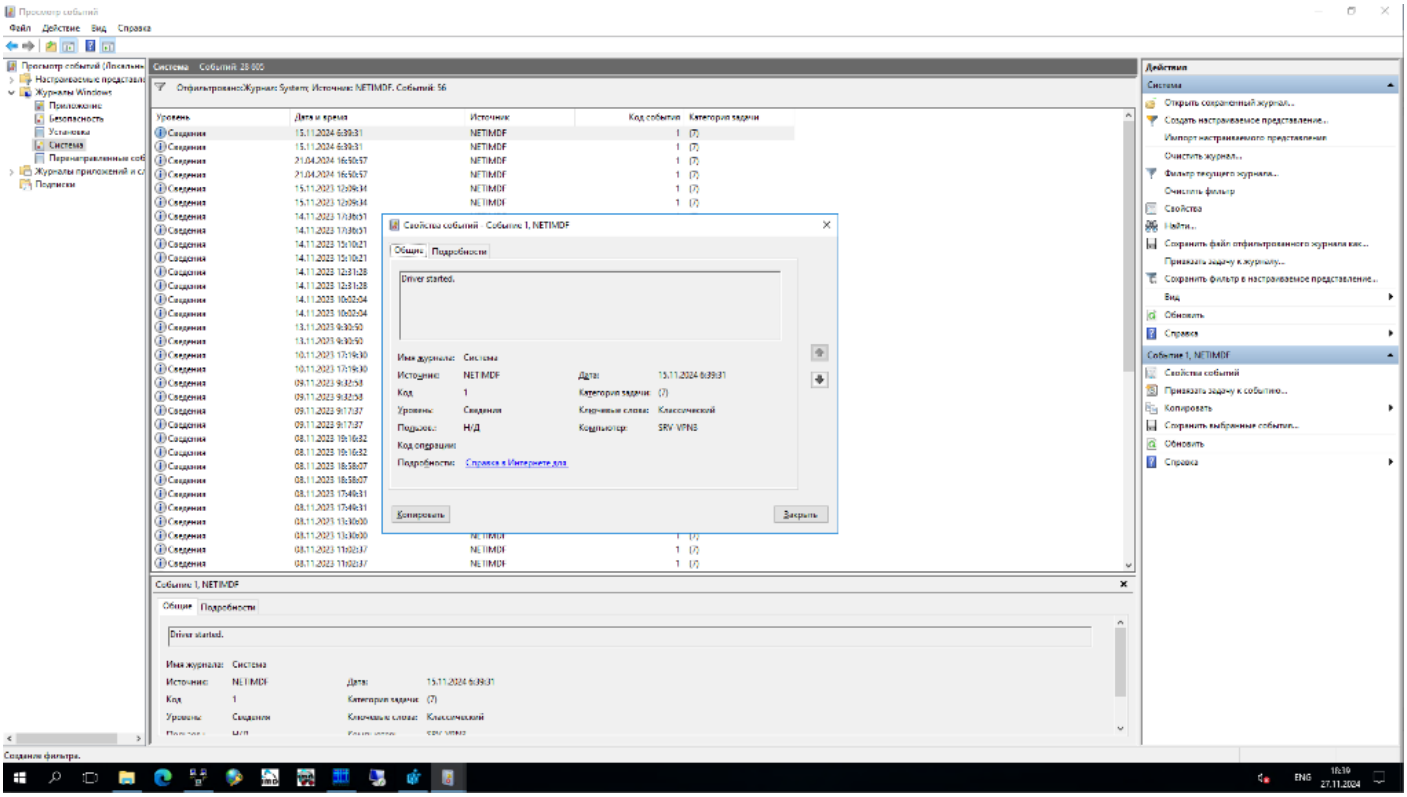

Рисунок 5 События в системном журнале Windows связанные с работой драйвера.

2.1. Настройка программного обеспечения для подключения к серверу.

Режим работы программного обеспечения, при котором применяются настройки, обеспечивающие взаимодействие по «закрытому» каналу с сервером, IP-адрес которого известен, можно назвать клиентским. Отличительной особенностью данного режима является отсутствие на сервере информации об IP-адресе клиента в записи списка клиентов.

Все данные программного обеспечения хранятся в файлах системного каталога %WinDir% (Обычно C:\Windows). Взаимодействие с файлами (чтение, запись, удаление) осуществляется, непосредственно, драйвером. Программа передает данные драйверу и получает их от него через команды на базе системных вызовов (IOCTL). Для рассматриваемого режима работы существует две группы настроек, сохраняемые в разных типах файлов:

- Настройки конфигурации, хранящиеся в файлах {имя файла}.cfg;
- Таблицы (списки) данных для подключения к серверам подключений, хранящиеся в файлах {имя файла}.srv;
- Дополнения к записям таблицы серверов подключений (Описание), хранящиеся в файлах {имя файла}_srv.def;

Имена файлам, в зависимости от вида данных, хранящихся в них, назначаются согласно правилам, приведенным в Таблице 6.

Таблица 6 Имена файлов данных программы

Вид данных	Параметры конфигурации	Таблица серверов	Дополнение к таблице серверов
Общие настройки для минипортов	default.cfg	default.srv	default_srv.def
Частные настройки для минипорта	{UID минипорта}.cfg	{UID минипорта}.cfg	{UID минипорта}.cfg

По поводу термина «UID минипорта» следует дать пояснения. В «дереве устройств» программы можно увидеть, что название каждого сетевого интерфейса через тире дополнено строкой в формате \DEVICE\{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX}. Значение в фигурных скобках и есть UID -уникальный идентификатор, который операционная система присвоила сетевому адаптеру (минипорту). Уникальность идентификатора обеспечена в рамках конкретного компьютера с установленной операционной системой.

Пример:

В «дереве устройств» есть сетевой адаптер Intel(R) Ethernet Connection (2) I219-LM - \DEVICE\{31F3FBB0-5B1F-4B02-9AF2-F00DD45AF2FA} (см. Рисунок 5). Тогда названия файлов данных для этого адаптера будут: {31F3FBB0-5B1F-4B02-9AF2-F00DD45AF2FA}.cfg, {31F3FBB0-5B1F-4B02-9AF2-F00DD45AF2FA}.srv и {31F3FBB0-5B1F-4B02-9AF2-F00DD45AF2FA}_srv.def. Уникальный номер этого устройства можно найти в реестре операционной системы Windows в разделе реестра для класса сетевых адаптеров, который имеет идентификатор - {4d36e972-e325-11ce-bfc1-08002be10318}.

Рисунок 6 Сетевой адаптер в списке

Сопоставление названия и уникального идентификатора, как видно, из Рисунка 6, произведено в ветке реестра \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}\001: параметром DriverDesc указано имя «Intel(R) Ethernet Connection (2) I219-LM», а параметром NetCfgInstanceId указан UID {31F3FBB0-5B1F-4B02-9AF2-F00DD45AF2FA}.

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». Для применения настроек – «Применить». Чтобы применить настройки из файла – «Перезагрузить».

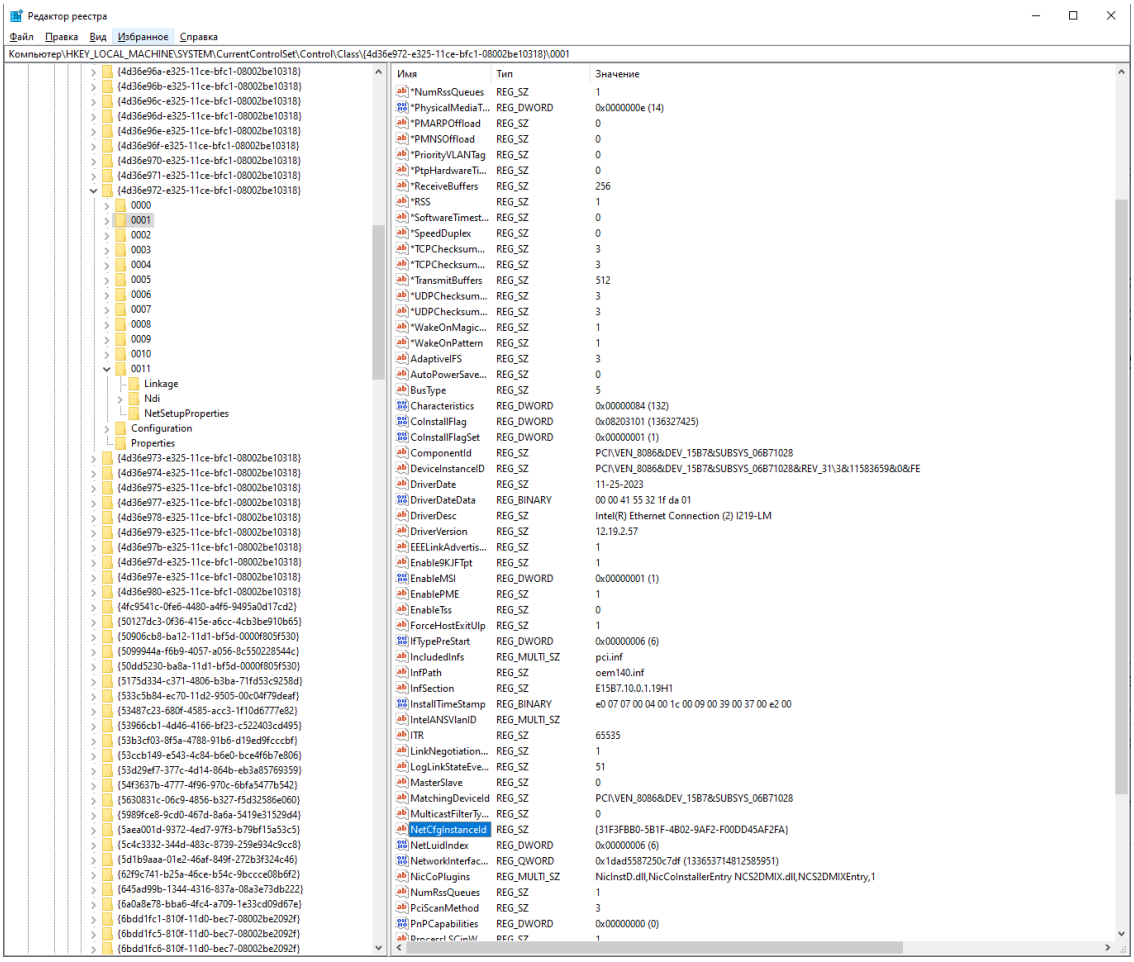

Рисунок 7 Сетевой адаптер в реестре Windows

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 преобразования.

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».

Возможно, если необходимо, изменить MTU для сетевых интерфейсов с помощью параметра «IP MTU» в контексте общих настроек или для конкретного сетевого интерфейса. В настройках по умолчанию MTU сетевых интерфейсов, обрабатываемых драйвером, уменьшен автоматически на 48 байтов. Они используются для задач инкапсуляции «закрываемых» протоколом драйвера пакетов.

Драйверу можно предписать иметь подготовленными (выделенными из оперативной памяти) определенное количество структур сетевых пакетов для ускорения процесса отправки и получения. Их количество по умолчанию – 5 для отправки и 5 для получения. С помощью параметров «Количество зарезервированных пакетов …» можно изменить это количество.

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 списке(таблице) серверов аналогичной информацией, за одним исключением: добавляется IPv4-адрес сервера или IPv4-адрес публикации сервера, если тот находится за маршрутизирующим оборудованием, выполняющим преобразование этого адреса в реальный адрес защищаемого интерфейса сервера.

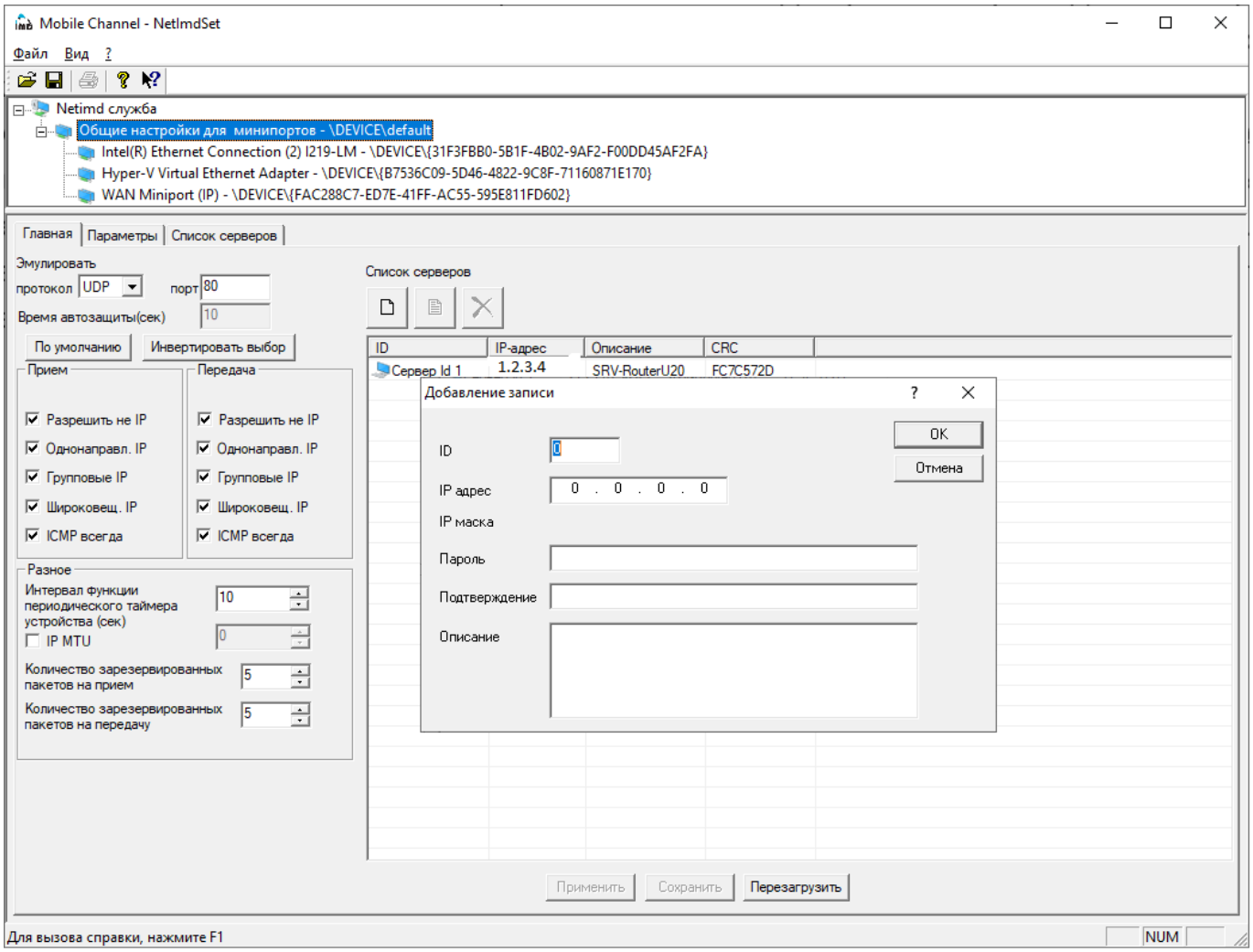

Рисунок 8 Контекст общих настроек

Записи в списке серверов можно добавлять, редактировать и удалять (см. Рисунок 7 и Рисунок 8).

Рассмотрим типовые операции в разных контекстах – для общих и частных таблиц (списков). Частные настройки имеют в драйвере приоритет перед общими.

2.1.4.1. Работа с таблицей серверов в контексте «Общие настройки минипортов».

Для добавления записи, необходимо нажать на кнопку «Создать запись», имеющую графическое изображение чистого листа, находящуюся под надписью «Список серверов». В появившемся модальном окне «Добавление записи» вносятся необходимые данные: идентификатор клиента (ID), IPv4-адрес сервера, ключевая информация (пароля, подтверждения пароля) и название (описание) сервера. После нажатия кнопки «Ок» в окне добавления записи, внесенные данные записываются драйвером в файл default.srv. Корректность ввода ключевой информации(пароля) можно определить по ее контрольной сумме, отображаемой в поле колонки «CRC» списка.

Для вызова формы редактирования записи, необходимо выбрать в таблице редактируемую запись и нажать на кнопку «Редактировать запись», имеющую графическое изображение заполненного листа, находящуюся под надписью «Список серверов». Редактирование записи, как правило, производится для корректировки или смены ключевой информации(пароля). После нажатия кнопки «Ок» в окне редактирования записи, внесенные данные записываются драйвером в файл default.srv. Корректность ввода ключевой информации(пароля) можно определить по ее контрольной сумме, отображаемой в поле колонки «CRC» списка.

Для удаления записи, необходимо выбрать в таблице удаляемую запись и нажать на кнопку «Удалить запись», имеющую графическое изображение наклонного красного креста, находящуюся под надписью «Список серверов». После подтверждения удаления (нажатии кнопки «Да» в информационном окне), данные удаляются драйвером из файла default.srv.

После перезагрузки компьютера, данные будет применены на всех адаптерах, для которых актуальна общая таблица серверов.

Для применения изменений в текущем сеансе, необходимо, перемещаясь по «дереву устройств», для тех адаптеров, использующих общие списки серверов, для которых необходимы новые данные, нажать кнопку «Перезагрузить»: произойдет замещение текущих списков серверов данными из файла default.srv для выбранного адаптера.

2.1.4.2. Работа с таблицей серверов в контексте конкретного минипорта (сетевого адаптера).

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.

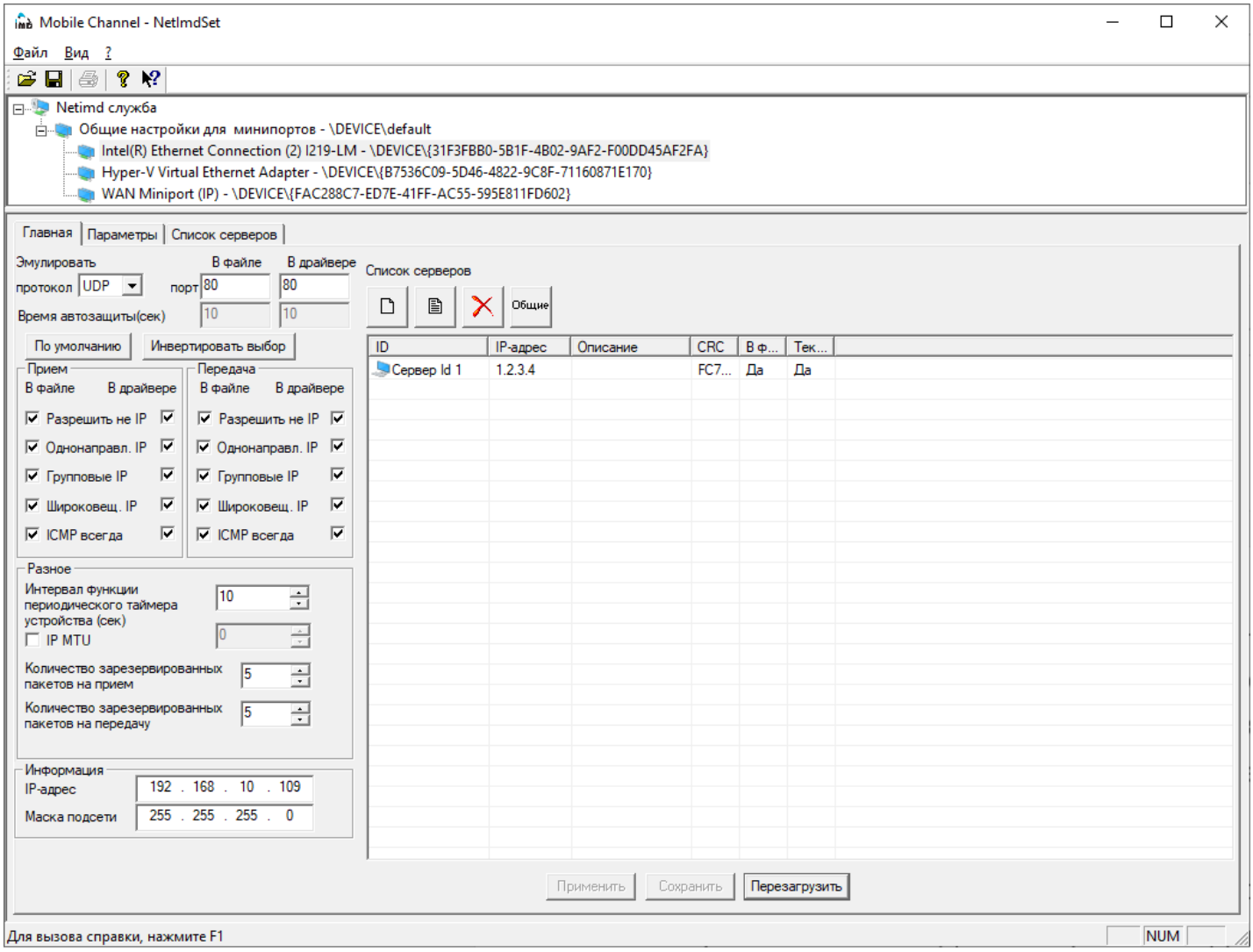

Рисунок 9 Контекст настроек для адаптера

Для добавления записи, необходимо нажать на кнопку «Создать запись», имеющую графическое изображение чистого листа, находящуюся под надписью «Список серверов». В появившемся модальном окне «Добавление записи» вносятся необходимые данные: идентификатор клиента (ID), IPv4-адрес сервера, ключевая информация (пароля, подтверждения пароля) и названия (описания) сервера. После нажатия кнопки «Ок» в окне добавления записи, внесенные данные записываются драйвером в файл {UID минипорта}.srv и вносятся в контекст выполнения для данного сетевого адаптера (используются в текущей сессии). Корректность ввода ключевой информации(пароля) можно определить по ее контрольной сумме, отображаемой в поле колонки «CRC» списка.

Для редактирования записи, необходимо выбрать ее в списке серверов и нажать на кнопку «Редактировать запись», имеющую графическое изображение заполненного листа, находящуюся под надписью «Список серверов». В появившемся модальном окне «Редактирование записи» вносятся необходимые данные. Редактирование записи, как правило, производится для корректировки или смены ключевой информации(пароля). После нажатия кнопки «Ок» в окне редактирования записи, внесенные данные записываются драйвером в файл {UID минипорта}.srv и вносятся в контекст выполнения для данного сетевого адаптера (используются в текущей сессии). Корректность ввода ключевой информации(пароля) можно определить по ее контрольной сумме, отображаемой в поле колонки «CRC» списка.

Для удаления записи, необходимо выбрать ее в списке серверов и нажать на кнопку «Удалить запись», имеющую графическое изображение наклонного красного креста, находящуюся под надписью «Список серверов». После подтверждения удаления (нажатии кнопки «Да» в информационном окне), данные удаляются драйвером из файла {UID минипорта}.srv и из контекста выполнения для данного сетевого адаптера.

3. Получение вспомогательной информации.

Для получения дополнительной информации о создаваемых соединениях используется программа NetImdStat.exe. С помощь данной программы можно визуализировать процесс соединения и параметры преобразования сетевых пакетов. Информацию об активных соединениях можно получить на вкладке «driver» данного приложения (Рисунок 10). Данные представлены в виде списка «Connections». Пояснения по колонкам данного списка сведены в Таблицу 7.

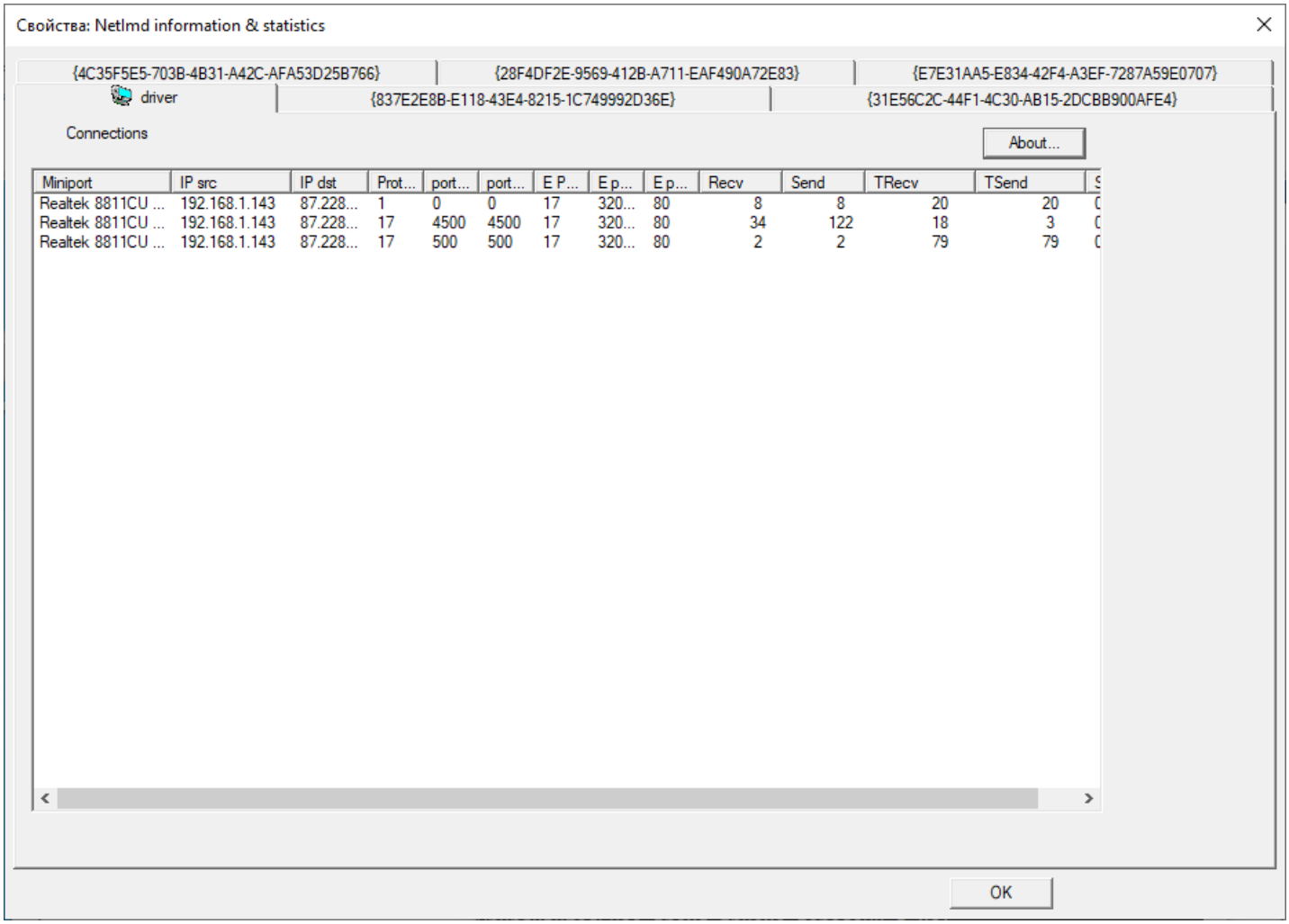

Рисунок 10 NetimdStat.exe - Отображение информации о соединениях.

Остальные закладки окна программы имеют названия, соответствующие уникальным номерам минипортов (сетевых адаптерах), контролируемых драйвером. Для каждого минипорта можно получить статистическую информацию о количестве обработанных драйвером пакетов с момента включения компьютера.

Таблица 7 Данные о соединении.

№ п/п	Название колонки списка	Описание
1	Miniport	Название минипорта (сетевого адаптера) локального компьютера, отправляющего/принимающего «закрытые» пакеты
2	IP src	IPv4-адрес минипорта локального компьютера (на котором запущена программа NetImdSet.exe)
3	IP dst	IPv4-адрес удаленного компьютера(хоста) или адрес его публикации в сети Интернет, с которым происходит взаимодействие или устанавливается связь.
4	Protocol	Реальный протокол взаимодействия с удаленным компьютером(хостом)
5	port src	Реальный порт источника локального компьютера (Используется только для протоколов TCP, UDP)
6	Port dst	Реальный порт приемника удаленного компьютера (Используется только для протоколов TCP, UDP)
7	E Protocol	Протокол эмуляции исходного пакета. При отправке, сетевой пакет инкапсулируется в пакет данного протокола с изменением типа протокола в IP-заголовке и новым заголовком данного протокола (Protocol -> E Protocol). При получении такого пакета производится обратное преобразование (E Protocol -> Protocol). По умолчанию задан протокол UDP (рекомендуется использовать для соединений через Интернет).
8	E port src	Порт источника локального компьютера, используемый для протокола эмуляции. На клиентских компьютерах (хостах), с которых осуществляются подключения к серверам может быть любым: равным реальному порту источника для реальных протоколов TCP и UDP или автоматически присвоенным драйвером.
9	E port dst	Порт приемника удаленного компьютера, используемый для протокола эмуляции. На клиентских компьютерах (хостах), с которых осуществляются подключения к серверам соответствует указанному в настройках для конкретного минипорта или, в случае отсутствия частных настроек, в общих настройках. По умолчанию порт 80.
10	Recv	Количество принятых сетевых пакетов в данном соединении.
11	Send	Количество отправленных сетевых пакетов в данном соединении. При превышении временного интервала между отправленными пакетами в 240 секунд, информация о соединении удаляется.
12	TRecv	Время в секундах, прошедшее с момента получения последнего пакета в данном соединении. При превышении временного интервала между полученными пакетами в 240 секунд, информация о соединении удаляется.
13	Tsend	Время в секундах, прошедшее с момента отправки последнего пакета в данном соединении. При превышении временного интервала между полученными пакетами в 240 секунд, информация о соединении удаляется.
14	Status	Статус TCP соединения, если Протокол эмуляции (E Protocol) – TCP.

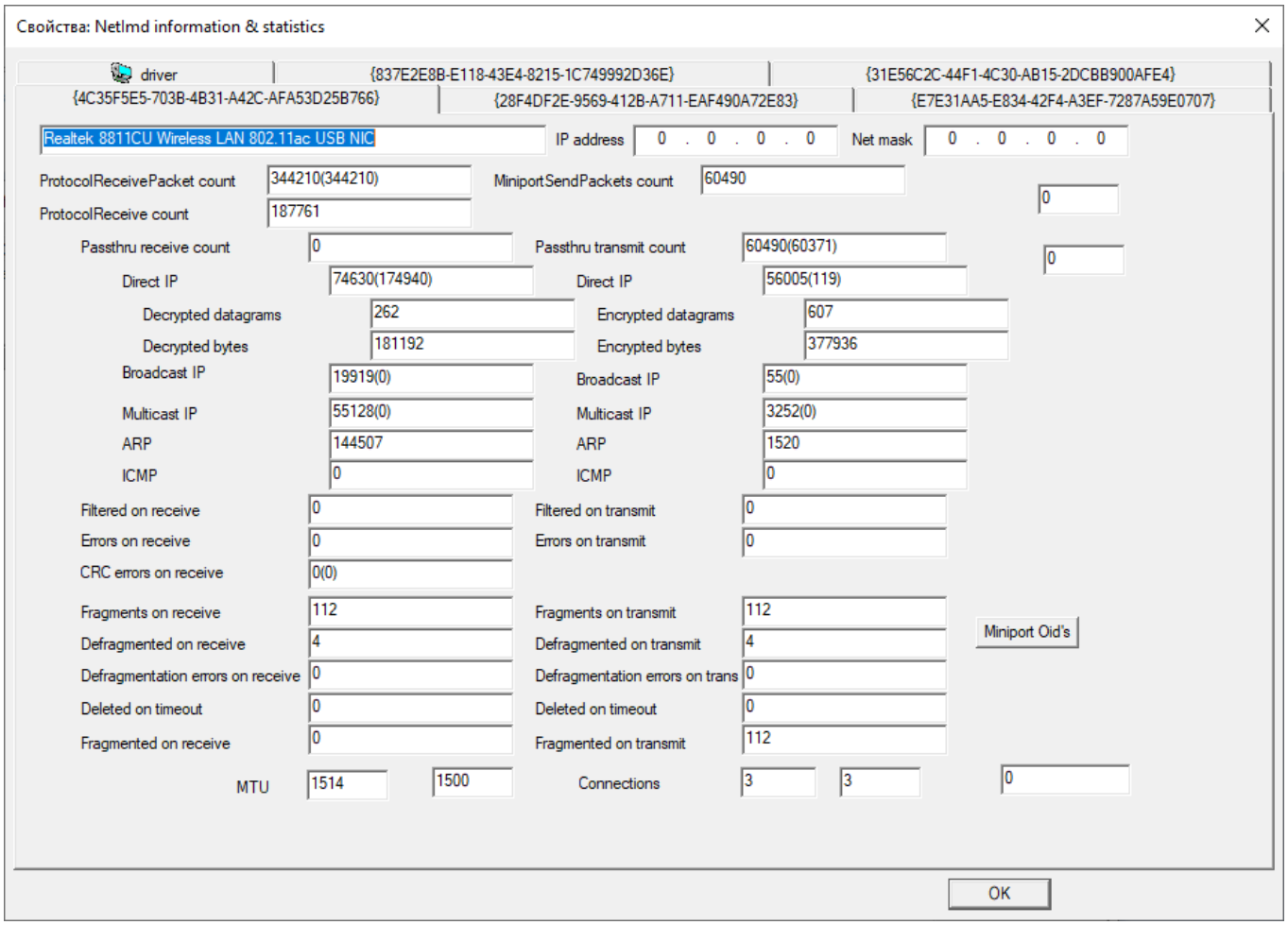

Рисунок 11 Статистическая информация по минипорту.

3.1. Настройка программного обеспечения для серверного режима работы.

Данному вопросу посвящен отдельный документ – Руководство Администратора Сервера подключений (Инструкция по развертыванию системы защищенных подключений на основе программного обеспечения IMDTech NETIMD MC).

3.2. Настройка программного обеспечения для режима работы туннеля.

Данному вопросу посвящен отдельный документ - Руководство Администратора Сервера подключений (Инструкция по развертыванию системы защищенных подключений на основе программного обеспечения IMDTech NETIMD MC).