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.

уро вен ь (La yer)	Наименование уровня OSI (OSI layer description)	тип данных (PDU)	Первичные задачи драйвера	деиствия драйвера при обработке исходящего трафика	деиствия драивера 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)	Cегменты (Segment s)	Анализ заголовков протоколов транспортно го 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

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

L2	Канальный уровень (Data link layer)	Байты (bytes)/ Кадры(fram es)	Анализ заголовков протоколов канального уровня (Ethernet 802.3,	незашифрованных пакетах Фильтрация на основе анализа Ethernet - заголовка	Фильтрация на основе анализа Ethernet - заголовка
			802.11,)		
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.

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

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 программаного 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».

A Molic Channel - NetImdSet					
Min Bay ?       Metind capacity      Metind capacity      Metind capacity      Metind capacity      Moniport (IP) - \DEVICE(Veff2956C-5046-4822-9C8F-7110871E170)      WAIN Miniport (IP) - \DEVICE(Veff2958C-5046-4822-9C8F-7110871E170)      WAIN Miniport (IP) - \DEVICE(Veff2958C-5046-4822-9C8F-7110871E170)      WAIN Miniport (IP) - \DEVICE(Veff2958C-5046-4822-9C8F-710871E170)      Wain Miniport (IP) - \DEVICE(Veff2958C-5046-488-4884-4822-9C8F-710871E170)      Wain Miniport (IP) - \DEVICE(Veff2958C-5046-488-4884-4884-4884-4884-4884-4884-48	Mobile Channel - N	√et/mdSet	-		×
Image: Source	айл Вид ?				
Metimic coyxis  Metimic coyxis <th>ê 🖬 🦽 🤋 🕅</th> <th></th> <th></th> <th></th> <th></th>	ê 🖬 🦽 🤋 🕅				
Compared Distance and Memorphics - UDVICCE (Lefender     Hyper V Virtual Ethermen Adapter - ODSVICCE(MAR22-9CBF-711987TE170)     Hyper V Virtual Ethermen Adapter - ODSVICCE(MAR22-9CBF-711987TE170)     Mathematical Etherment Adapter - ODSVICCE(MAR22-9CBF-711987TE170)     Mathematical Etherment Connection (2) (2) 5-UM - UDEVICE(3) 535880-381T-4802-3A72-F000D45A52FA)	Netimd служба				
• hyper-Virtual Ethernet Adapter - DEVICCI (37156706-700-7046-4822-9267-71108771E70)           • Warth Minpart (IP) - UDEVICE (472387-0706-704F-4802-9472-F000D45472FA)           Sautors. poppawery naponer           • Perincipaasia cobinnit           • Varpoketton y papanetesia           • Outdool           • Metery napones           • Perincipaasia cobinnit           • Varpoketton y papanetesia           • Depreprezentesia           • Heegonause           • Metery napones           • Perincipaasia cobinnit           • Varpoketton y papanetesia           • Respectation of galately           • Metery napone           • Respectation of galately	🖻 🐚 Общие наст	тройки для минипортов - \DEVICE\default			
WAN Miniper (IP) - VDEVICE((FAC2867-ED/E-AFC5-5958E11FD602)         Intel(R) Ethernet Connection (2) [219-LM - VDEVICE((31F3F880-381F-4802-38472-F00DD45AF2FA)         Sauturus propression propose         Principaase columitation         Vistophages columitati	Hyper-V	Virtual Ethernet Adapter - \DEVICE\{B7536C09-5D46-4822-9C8F-71160871E170}			
	🐚 WAN Mir	niport (IP) - \DEVICE\{FAC288C7-ED7E-41FF-AC55-595E811FD602}			
Защитить программи пролеми         Сменяль пароль.           -Percenguaue colorinit		themet Connection (2) I219-LM - \DEVICE\{31F3FBB0-5B1F-4B02-9AF2-F00DD45AF2FA}			
Защинть программи паролем         Симисть пароле           Principaara cofornit					
Защинть программу паролем         Сименть пароль           Penicipaaus colonitititity					
Защитить программи пароле         Сменять пароль           Регистражия собитий         Устройство управления           © Quadiou         Скаче           © Певдпреждения         Сменять пароль           Сменять пароль         Секенть пароль           Интерритиратися         Скаченть пароль           Скаче         Активно           © Певдпреждения         Сменять пароль           Сменять пароль         Сменять пароль           Интерритиратися         Сменять пароль           Интерритиратися         Сменять пароль           Пародотария         Сменять пароль           Теве         72002           Stas         110115           Stas         110115           Stas         110115           Соронски         КТОР ОК           Соронски         КТОР ОК           Соронски         КТОР ОК           Соронски         1158.21           Редоскийском         1158.22           Перезориком         NETIMOF SYS           Оргонски         NETIMOF SYS           Сороронски         1158.21           Перезориком         NETIMOF SYS           Оргонски Перезориком         NETIMOF SYS					
Peruntapaan cookinnii Peruntapaan vaita paanevaa Anteena papois Peruntapaan cookinnii Vorpaanevaa Anteena Porpaginge xaeena Veegonauvaa Ceesonavoe exasaavee NNDISIMDS Netophauvaa gaateepe Habaanee Contensione exasaavee NNDISIMDS Tene 72002 See 115016 Internatione NETIMO FSYS Rebeaturd of the NETIMO FSYS	<b>F</b> 2	Commence of the second s		-	
Principality and columnial          — "Orpotation of pagesnesses             ✓ Outdoors           Campo - Antineso             ✓ Incorpore ageins           Campo - Antineso             Fle           Coll Moders             Comportageins           Comportageins             Company have           Not Strip             LagaCompit           NetTIMDE Sris             LagaCompit           Company have             Lignologing           Lignologing             LagaCompit           Loging             Company have           NETIMOF Sris             Company have           NETIMOF Sris             Company have           NETIMOF S	защитить програм	иму паролем Сменить пароль			
Ф Ошибии         Статус         Активно           Ф Педадреждина         Синопное название         \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	<ul> <li>Регистрация событи</li> </ul>	<sup>10</sup> Устройство управления			
	Ошибки	Статус Активно			
Сонтрольника         Сонтрольное название         NUNDISIMDS           Назване         Заничние         Поличние         Поличние           Назване         Заничние         Поличние         Поличние           Работо сонтрольной         Сонтрольной поличние         Поличние         Поличние           Работо сонтрольных о драйвере         Поличние         Поличние         Поличние         Поличние           Работо сонтрольных о драйвере         Поличние         П	🔽 Предупрежден	108			
Prepagative         Description         F1 Microarce           Microprisation or galaxiesce					
Metopotausis o gaabappe Hasasave 3-sovence File C.VMrobovi System 32-driven'ivetimit ays Date 7:20019 Date 1:20019 See 1:10016 Internatione NETIMDE SYS ProductName NETIMDE SYS ProductName IMDTech LLC, Pasia LagaCompity Name IMDTech LLC, Pasia Lag	Информация	Cambolibhue Habbanite			
Информация а драйвере					
Metophagura o galetepe       File     Sevenses       File     CVMsdows System 32-drivers' vetimatilitys       Defe     19/9 2019       Time     72002       Size     11015       Internatione     NETIMOR SYS       ProductName     MCTable LC Lastas       CompanyIname     MCTable LC Lastas       ReDeadstreame     NETIMOR SYS       Rebestotion     Nas Reb Diver MC       ReVension     1138 21       OrganaFilename     NETIMOR SYS					
Информация о дравере Название Пе С:Windows: Date 19.05.019 The 2.20.02 Network/Name NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS PeduatName NETIMOFSYS Copposition 119.8.21 PeduatName NETIMOFSYS					
Anaparety         Susterie           File         C:\Windows\ystem32:drivers\vetmdf.sys           Date         19.05.2012           Starelitane         116016:5.5'5           ProductName         MDTech LLC, Rasis           LegaCopright         Copper/Int           ProductName         NETIND MC           ProductName         NETIND FS           Disposition         138.21           ProductName         NETINDF SYS	Информация о врайве	ne .			
The server         C:Windows Option 32 driven's retend bys           Defe         19/9 2019           Time         72002           Size         115016           International Mark         FEITIMOR SYS           ProductName         NETIMOR SYS           OrganaFilename         NETIMOR SYS					
Date         19.07.2019           Time         7.20.02           Sas         110.016           Sas         110.016           PoductName         NDTS-NT           LegiCophylit         VETIMO DVS           CompanyName         MDTS-th LC, Russi           LegiCophylit         VETIMO DVS           ProductName         NDTS-th LC, Russi           LegiCophylit         VETIMO DVS           ProductName         NDTS-th LC, Russi           LegiCophylit         VETIMO DVS           OrganaFilename         NETIMOF.SYS	File	C:\Windows\System32\drivers\netimdf.svs			
The 22002 Size 118016 Hetmatakane NETIMD MC CorporyName MIDTech LLC Reases LegaCorport Copyright (C) 5F 2005-2019 ProductVersion Nas Ref Driver MC FilePestoption Nas Ref Driver MC FilePestoption Nas Ref Driver MC FilePestoption NeTIMDF SYS	Date	19.09.2019			
Decontinent NETIMOFSYS Produktione NETIMOFSYS Corporation Co	Time	7:20:02			
Productiveme NETIMD IAC CompanyName IMTCeh LC, Rasta LegaCopright C Spright (C) SF 2005-2019 Productivemon 1198.21 RieDescription Nids Filer Driver MC FileVenton I.198.21 OrginaFilename NETIMDF SYS	InternalName	NETINDE SYS			
CompanyName IMOTech LLC, Russia LegaCoxynght LegaCoxynght FS 2005/2019 PhodudYearon 1158.21 ReVersion 1158.22 OrginaFilename NETIMOF.SYS	ProductName	NETIND MC			
LegaConjrdt C. Corpit E, SF 2005-2019 PrioCestration 1198.22 PrioCestration Niss Rev Diver MC PreVenano 1198.22 OrginaFilename NETIMOF SYS	CompanyName	IMDTech LLC, Russia			
FRU-Davidshin Nika Far Diver MC. FRU-Varian 1138.21 Orgina/Filename NETIMOF.SYS	LegalCopyright	Copyright (C) SF 2005-2019			
TevNexion 119.821 OrignalFiename NETIMDF.SYS	Product version	1.13.8.21 Nile Der Diver MC			
Corporation NETIMDESYS	FileVersion	19821			
Соранль	OriginalFilename	NETIMDF.SYS			
Соранть					
Сорвиль					
Соразль					
сорекив		Counsiem			
		Сохранить			
	1		_		

Кроме того, предоставлена возможность выбрать, события какого уровня важности будут регистрироваться работе при 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 peecrpa 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%\SystemRoot%\SystemRootOC.

🔡 Редактор реестра					_	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид <u>И</u> збранное <u>С</u> правка						
	^	Имя	Тип	Значение		
. NETIMDF		ab) (По умолчанию)	REG_SZ	(значение не присвоено)		
NetJoin		ab EventMessageFile	REG_EXPAND_SZ	%SystemRoot%\System32\netimdfx64.dll		
Netlogon	$\sim$	100 TypesSupported	REG_DWORD	0x00000007 (7)		
< >>	>				 	
Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\C	Curren	tControlSet\Services\EventLog\System\NETIMDF				

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

Фильтровать текущий	і журнал
Фильтр XML	
Да <u>т</u> а:	Любое время 🗸
Уровень события:	<u>Критическое</u> Предупре <u>жд</u> ение Подро <u>б</u> ности
	Ощибка Сведения
По журналу	Журнал <u>ы</u> событий: Система
🔘 🛛 о источнику	Источники событий: NETIMDF
кодов, разделяя их 1,3,5-99,-76	запятыми. Для исключения условия введите знак минус. Например: <Все коды событий>
Категория задачи:	<b>v</b>
Кл <u>ю</u> чевые слова:	<b>•</b>
Подьзователь:	<Все пользователи>
Ко <u>м</u> пьютеры:	<Все компьютеры>
	Ощистить
	ОК Отмена

Рисунок 3 Фильтр для системного журнала Window

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

атр событий (Лосалын-	Система Событий 28-805						Aevictore
странваемые представля	7 Отбальтровно:Жарнал	System: Honoweak NETIN	10F. Cotivensk 56				Cacrana
Discourses		1 C C					<ul> <li>Ompure corporement sypnam.</li> </ul>
Genome concerns	Уранны	Дата и время	Источник	Kog coleman Kateropan sagean		^	COURTS HALTINA MANUE REPAILTMONICH
Успановка	Остадотия	15.11.2024 6:39:31	NETIMOF	1 (7)			Variable - ACTUARIANALS DEPARTMENT
CHCTEMB	Останова	15.11.2024-6:39:31	NETIMOF	1.0			Comment of the local division of the local d
Theparturpation and a Col	Осидная	21.04.2024 16:50:57	NETIMOF	1 0			
Carlor of the second se	(I) Cardineau	21042024169897	NETIMOR	1 10			Y waterp to gatern symptome.
	(I) Cantineau	15.11.2023 1209634	NUMBER	1 10			Очистить фильтр
	(i) Contraction	141120231209534	142115424	1.10			CaoAcrea
	(I)Correction	1411-2021 1208-01	Casificina columnii - Columne I, NETIMDE		×		We Hatte.
	(I) Cocachina	14.11.2023 15:10:21					🔓 Сорнить файл отфальтраканного хурнала ка
	(I) Catalores	14.11.2023 15:10:21	Souther Landborners				Призналь задачу к журналу
	Осасдания	14.11.2023 12:31:28	Dever materia				
	Осацияни	14.11.2028 12:31:28					A CONTRACTOR OF A CONTRACTOR O
	Спарния	14.11.2023 10:02:04					544
	Campoon	14.11.2023 10:02:04					C Cleans
	Остана	12.11.2023 908250					Cripters
	Dennes	10.11.2023 929290			4		Colores 1 MCIARDE
	() Carterian	10.11.2023 12:19:30	Man Approval Caciona		121		
	ОСтедения	09.11.2023 9:32:58	Истодник: NET MDF	(Agrai 15.11.2024 6/39/31	4		Carvena conuma
	Сандиная	09.11.2023 9:32:08	Keg 1	Кадегория задечи: (7)			Призизать задачу к себытико
	Осседения	09.11.2023 9/17:37	Урожены: Свядения	Клерчиные слова: Классамиский			Rig Konvposate
	ОСосдения	09.11.2023 9:17:37	Reputer HG	Kommunitip: SRV VPNG			🔛 Стеринить выбранные событил
	Осасдания	08.11.2023 19:16:32	Kog crephyrer				C CONCEVED
	(I) Catgaries	08.11.2025 19:10:52	Departmenter Conservation				Concerca.
	Останов	08.11.2025 18:58:07	contraction (construction of the				
	OCHIMAN	08.11.2023 12.49-31					
	() Common	08.11.2023 1749-31					
	(i) Conserver	08.11.2023 13:30:00	Konsponse	1	acpure		
	(I) Congresses	08.11.2023 13:30:00	NUMBER	1.12			
	ОСведения	08.11.2023 11:02:37	NETIMOF	1.02			
	Оставния	08.11.2023 1102:37	NETIMOR	1 02			
	Column 1, NETIMOF					×	
	Общие Подробности						
	Driver started.					Î	
	Иникионала: Система						
	HETENNIC NETMOR	(lana)	1571232460901				
	Kee 1	Kereron	(7)				
		Cathering .					
	Уровена: Сведения	Koro-ka	Sectore: Maccinectia				
	Harrison Mrtt	Press of	CEN VIEWS				

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.

ல் Mobile Channel - NetImdSet	- 🗆 🗙
Файл Вид ?	
📽 🖬 🧔 🔋 🕺	
Wetimd служба     OfGuue настояки для минипортов • \D     Intel(R) Ethernet Connection (2) I219-LI     Hyper-V Virtual Ethernet Adapter - \DE     WAN Miniport (IP) - \DEVICE\[FAC288;	VICEOREMU M - IDDVCE [1915F860-581F-4802-962F-200DUSA2FA] //CEU[9736C09-5046-4822-962F-71160871E170] //CEUT2-41FF-AC5-59581E1F0002]
Главная Параметры Список серверов	
Заулародала протикал (UOP — порт 10) Векен аптозицити/сек) По уколечие Инверторать выбо Прием Разрешить не IP Г Одночагравл. IP Г Одночагравл. IP Г Груповые IP Г Г Притовые IP Г При	Списот серевроя
	Применить Сохранить Перезагрузить
Іля вызова справки, нажинте F1	NUM

#### 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.

🚵 Mobile Channel - NetImdSet								-		×
Файл Вид ?										
🖆 🖬 🏐 🕈 📢										
<ul> <li>Polyteind служба</li> <li>Oбщие настройки для минипортов - \DE</li> <li>The last state of the last</li></ul>	VICE\default 1 - \DEVICE\{31F3FBB0 ICE\{B7536C09-5D46- 7-ED7E-41FF-AC55-59	)-5B1F-4B02 4822-9C8F- 5E811FD602	-9AF2-F00DD45/ 71160871E170} !}	AF2FA}						
Главная Параметры Список серверов										
Змулировать В файле В драйвере протокол UDP • порт 80 80 Время автозащиты(сек) 10 10	Список серверов	Общне								
По умолчанию Инвертировать выбор	ID	IP-адрес	Описание	CRC	Βφ	Тек				
Прием Передача	Scepsep Id 1	1.2.3.4		FC7	Дa	Дa				
в фаиле в драивере в фаиле в драивере	-									
✓ Разрешить не IP										
🔽 Однонаправл. IP 🔽 🔽 Однонаправл. IP 🔽										
🔽 Групповые IP 🔽 🔽 Групповые IP 🔽										
🔽 Широковещ. IP 🔽 🕼 Широковещ. IP 🔽										
🔽 ІСМР всегда 🔽 🔽 ІСМР всегда 🔽										
Pasuoa										
Интереал Функции периодического таймера устройства (сек) ПР МТU										
Количество зарезервированных 5										
Количество зарезервированных 5 +										
Информация										
IP-agpec 192 . 168 . 10 . 109										
Маска подсети 255 . 255 . 255 . 0										
	1	ſ	Трименить С	охранить	Пере	загрузи	пь			
Для вызова справки, нажмите F1									NUM	

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.