

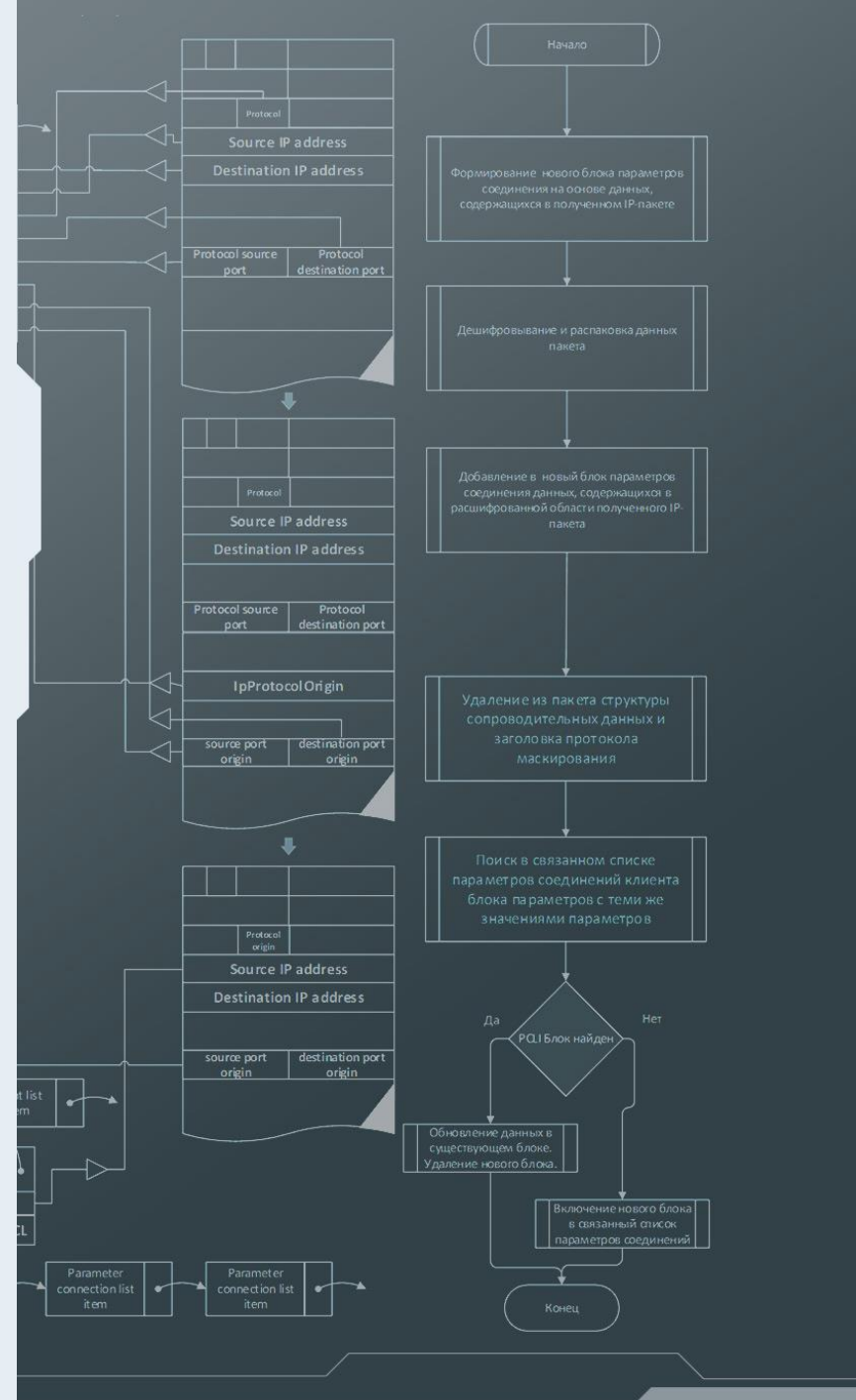
imdtch

Netimd: от кроссплатформенного
решения к аппаратному встраиванию

Задача.

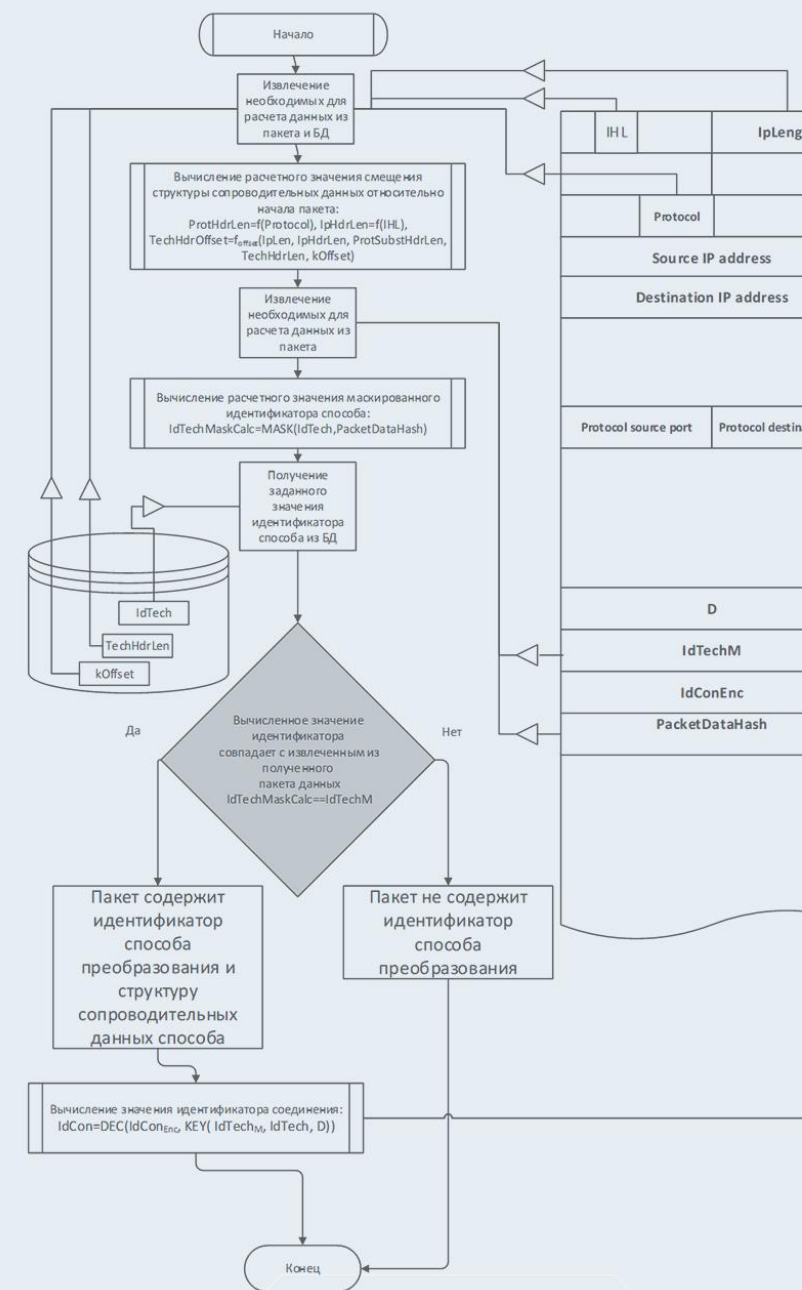
В связи с необходимостью защиты конфиденциальной информации, передаваемой по коммуникационным сетям общего пользования Internet потребовалось разработать программное обеспечение, которое было бы в состоянии:

- обеспечить защищенное соединение в сети Internet между мобильными компьютерами и корпоративной сетью через серверы удаленных подключений.
- Обеспечить защищенное соединение между географически распределенными подразделениями предприятия.
- Обезопасить сервера удаленных подключений от обнаружения и атак хакерами.



Решение.

Создано кроссплатформенное решение основанное на использовании собственного протокола обмена данными с алгоритмами симметричного шифрования — Netimd.



История.

Данная работа является логическим продолжением развития направления, по которому в ООО “ИМДТех” велись работы в течении последних лет. За это время были созданы следующие совместимые с новым решением программные продукты:

- Netimd для операционных систем Microsoft Windows 98SE/NT/XP/Vista/7/10 и серверных версий Microsoft Windows Server 2003/2008/2008R2/2012/2016/.. .

- Для ранних операционных систем решение выполнено на базе разработанного драйвера согласно спецификации [NDIS intermediate network driver](#). В дальнейшем был разработан [NDIS Filter Driver](#). Его использование началось с Windows 7/ Windows Server 2008.

- Netimd для Apple MacOS версий 10.4 - 10.15.4. Решение было выполнено на базе разработанного модуля ядра спецификации [Network Kernel Extension](#) типа [Interface filter](#).

- Netimd для различных версий операционных систем на базе Linux в виде [модулей расширения ядра](#).

Новая разработка на базе устройств с аппаратным встраиванием.

Преимущество — не нужно заниматься установкой программ. Остается только настроить устройство под конкретную задачу.

Подходит для



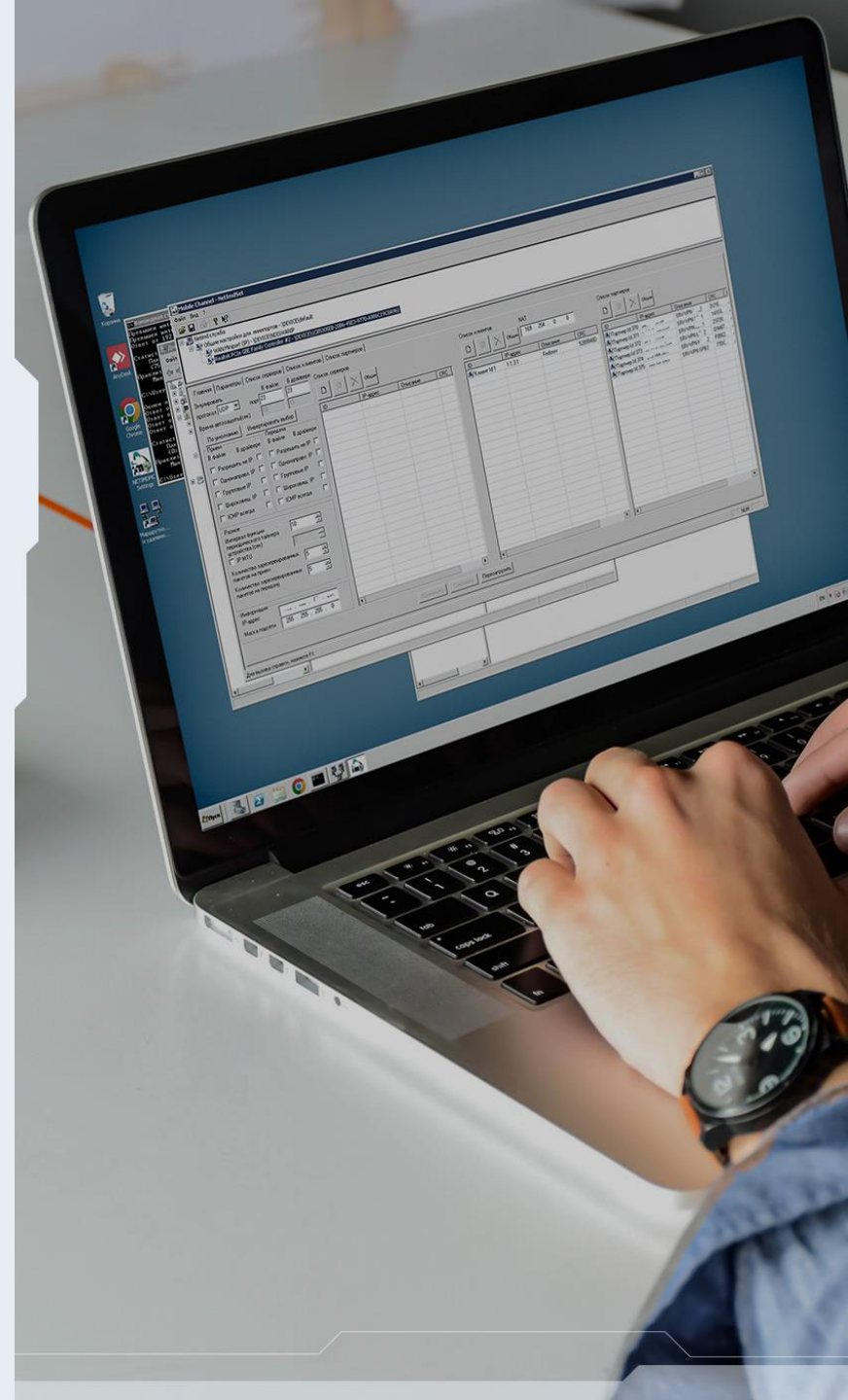
Microsoft Windows



Apple MacOS



Linux



Применение.



Обеспечение защищенного доступа к внутренним информационным ресурсам локальной сети сотрудникам предприятия, работающим дистанционно.



Возможность защищенного обмена информацией между отдельными компьютерами в локальной сети или сети Интернет.



Защищенное взаимодействие с «облачными» информационными ресурсами предприятия, размещаемыми в центрах обработки данных (ЦОД).



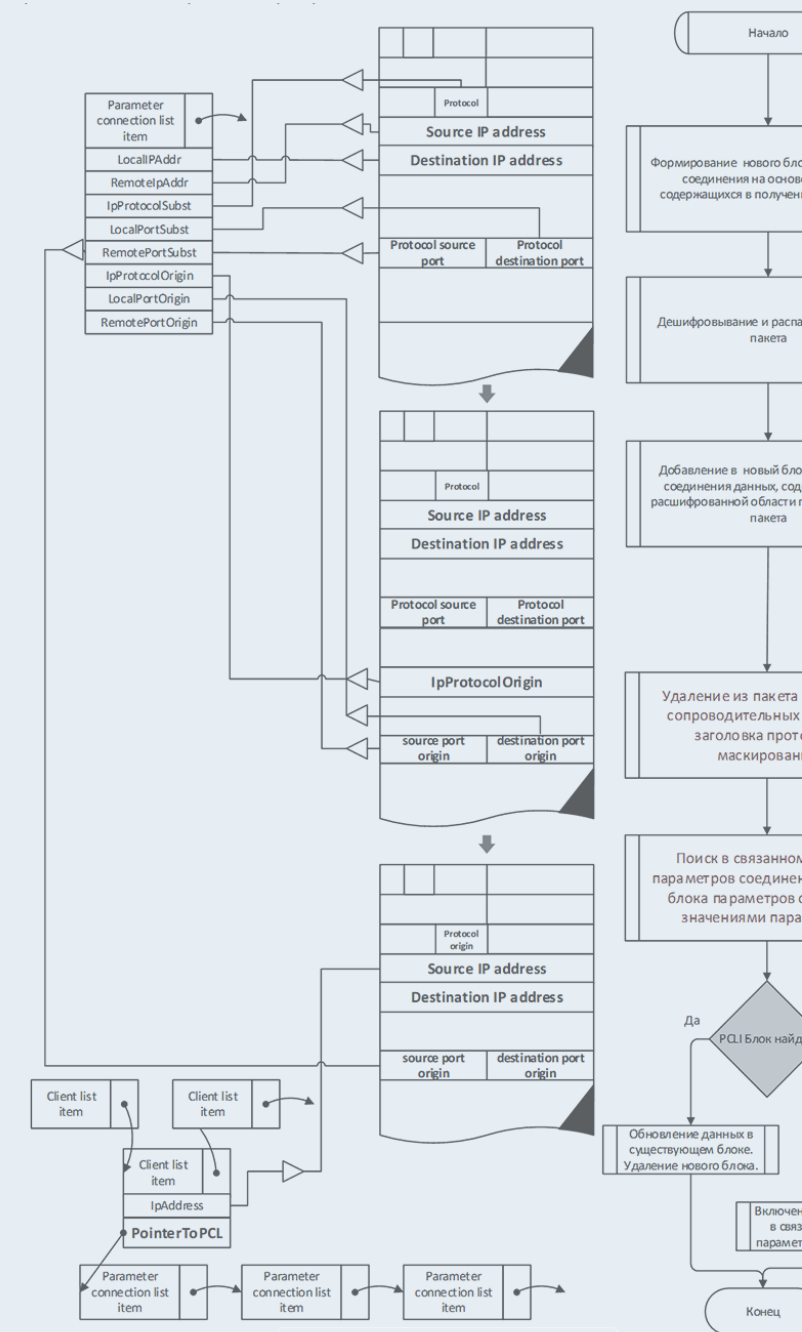
Интеграция с системой мониторинга объектов с обеспечением криптографической защиты канала обмена данными.



Использование для защиты систем дистанционного управления и контроля, например системы «Умный дом».

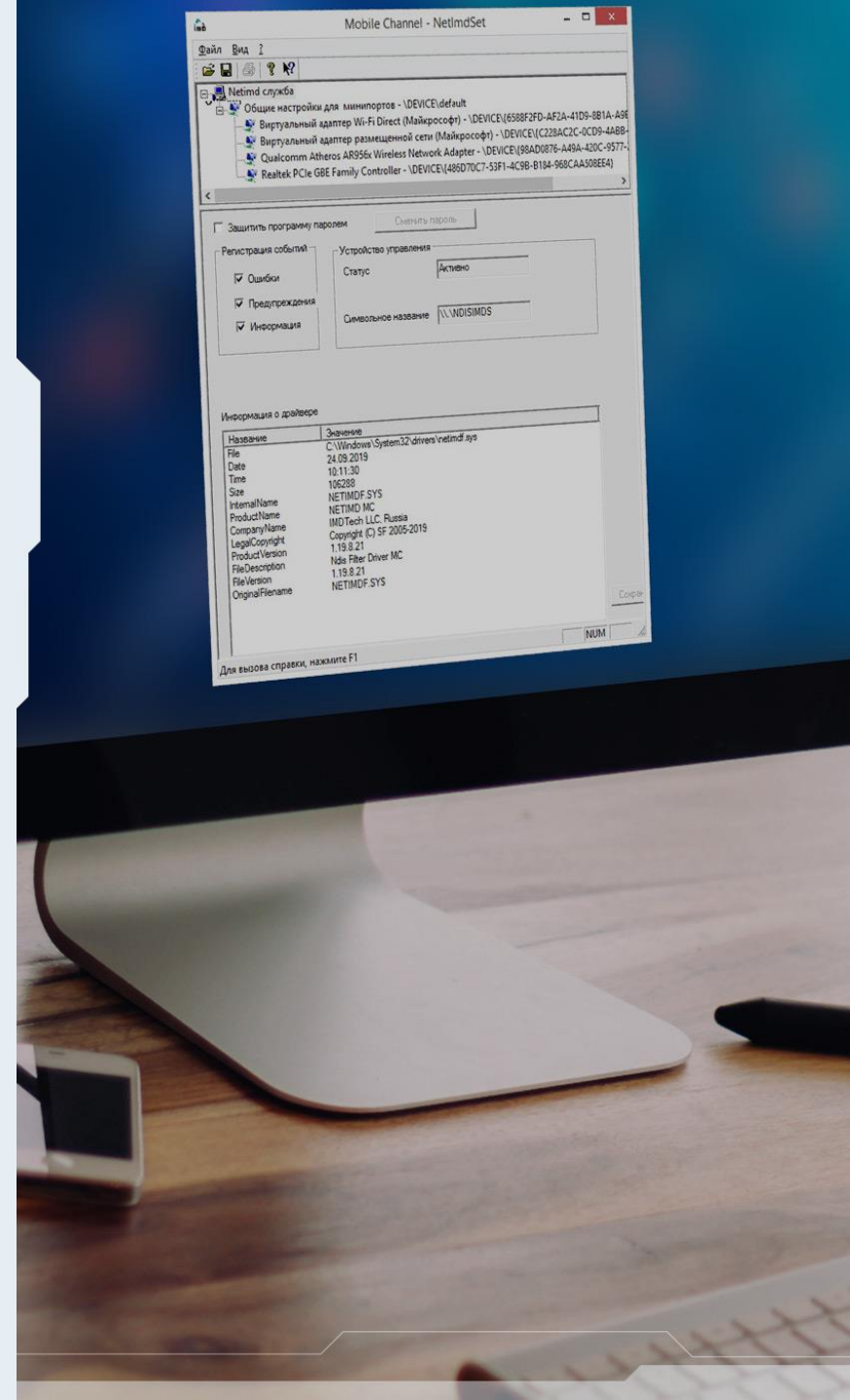


В системах дистанционного взаимодействия с движущимися объектами, для защиты информационных каналов управления и мониторинга.



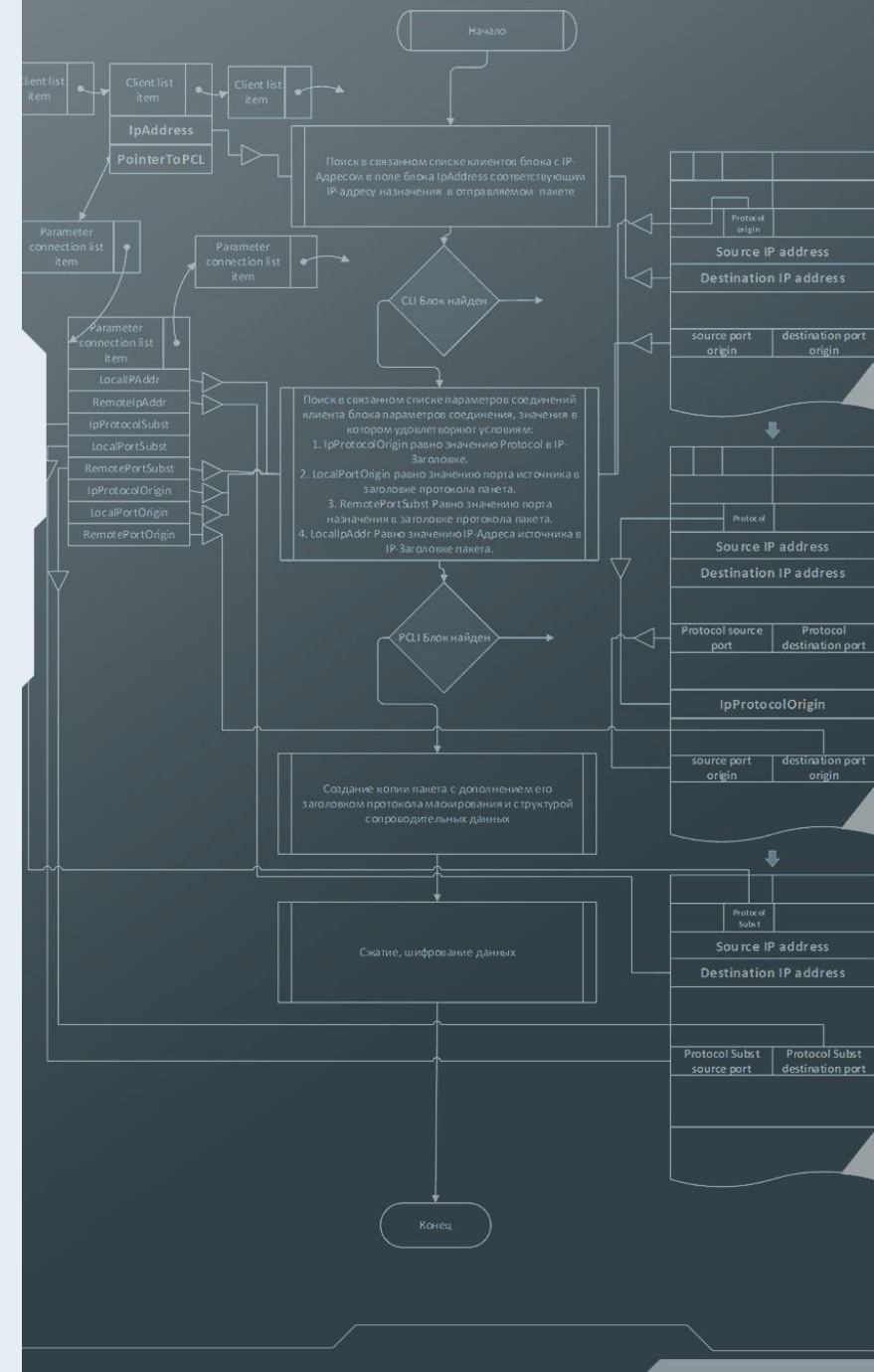
Функциональные возможности.

- Собственный протокол приема-передачи информации.
- Защищенное хранение ключевой информации на внешнем носителе USB.
- Обеспечение связи в режиме клиента, т.е. инициатора защищенного соединения.
- Обеспечение связи в режиме сервера, т.е. обработчика запросов клиентов.
- Обеспечение связи в режиме туннеля, т.е. соединение может устанавливаться по инициативе любой из сторон.
- Поддерживается режим работы криптошлюза в котором роутер будет передавать и принимать через «внешние» интерфейсы только обработанные собственным протоколом сетевые пакеты.



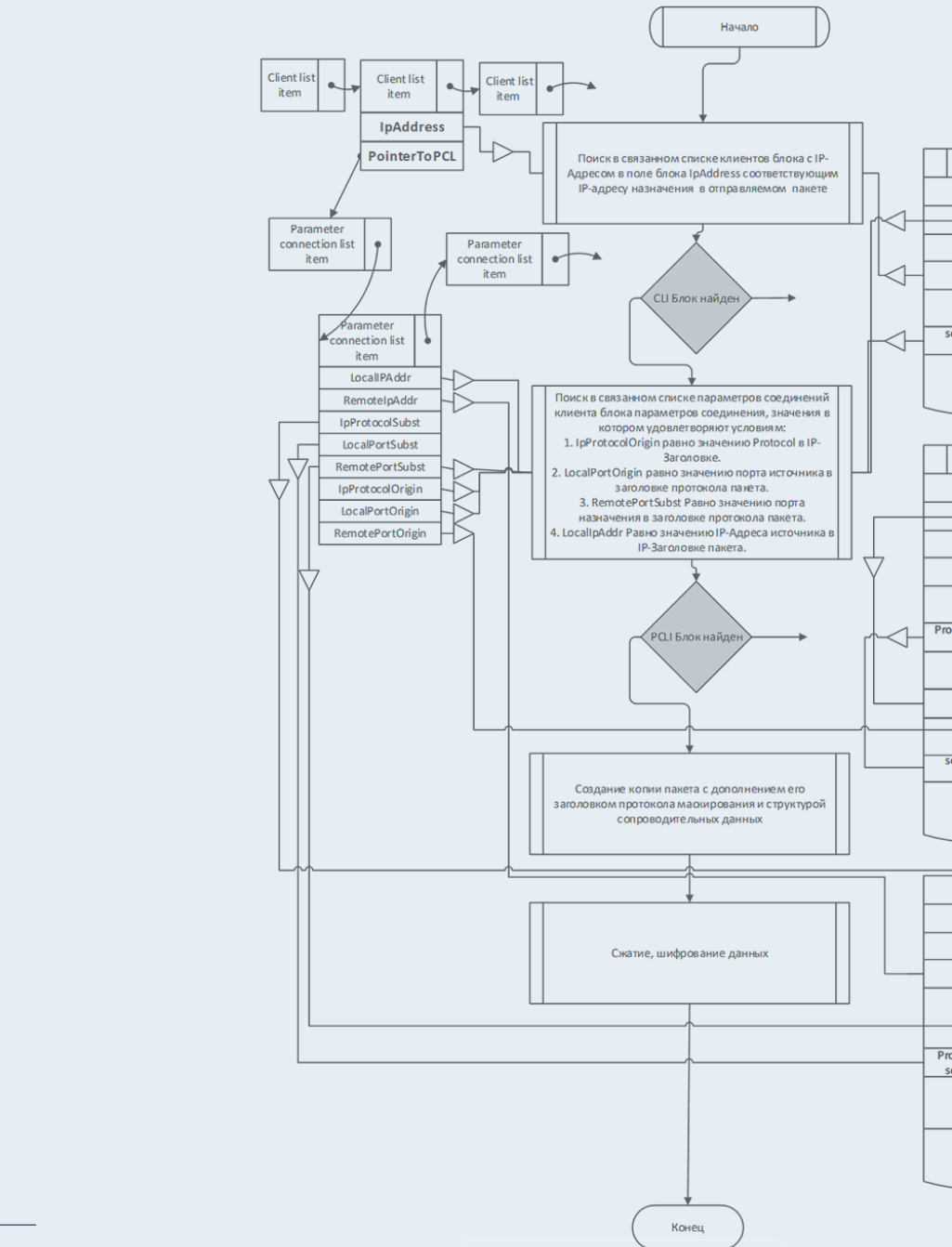
Отличительные особенности решения.

- Основой решения является динамически подгружаемый модуль ядра операционной системы [KeeneticOS](#), созданной в свою очередь на базе ядра Linux.
- Модуль контролирует весь поток пакетов Ethernet, проходящих через внешние интерфейсы (WAN) роутера. Выполняет, в соответствии с настройками, фильтрацию и модификацию пакетов.
- Модуль запускается автоматически при включении.
- Ключевая информация и программное обеспечение Netimd размещаются на USB флэш-накопителе малого размера и малой емкости (от 128 Мб), подключаемом к роутеру.
- В случае необходимости, программное обеспечение Netimd может быть размещено во внутренней Flash-памяти устройств Keenetic.
- Ключевая информация хранится в зашифрованном виде.
- Программное обеспечение Netimd «привязано» к оборудованию.
- Сохраняется возможность установки обновлений KeeneticOS для устройств Keenetic.



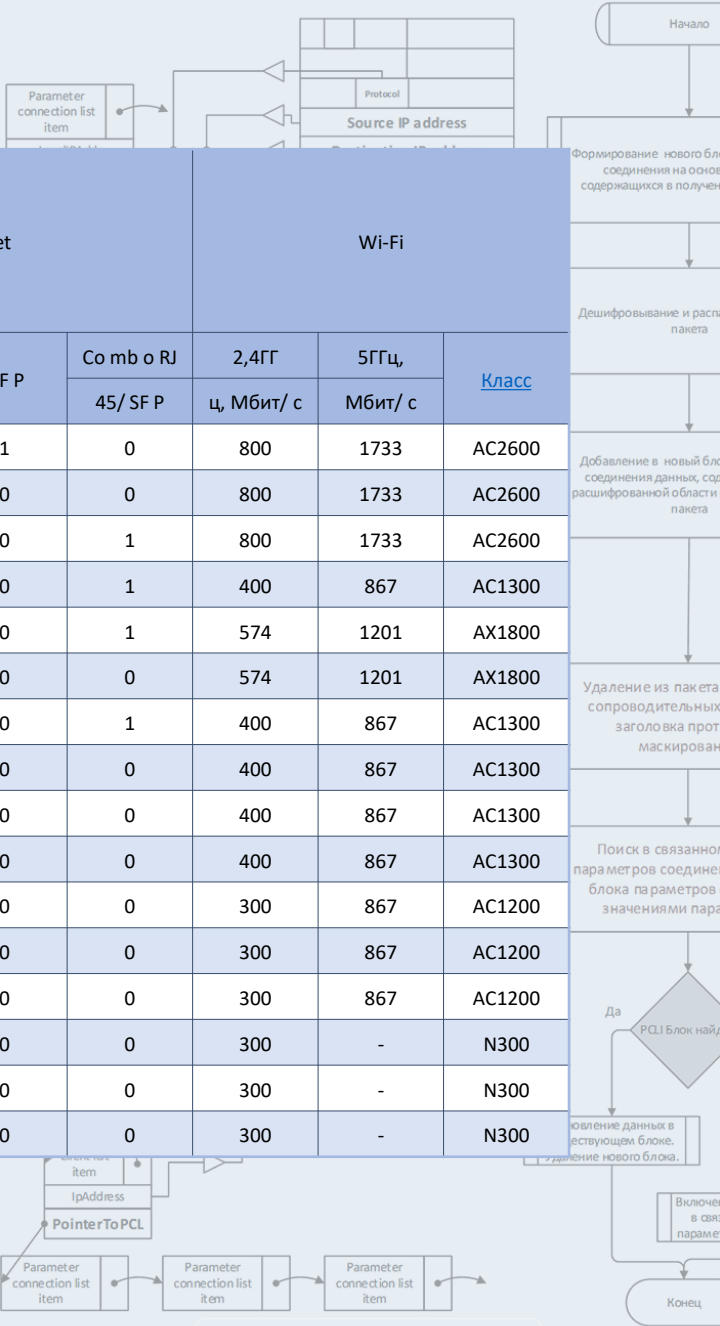
Почему выбрано оборудование Keenetic?

- Оборудование доступно в России и допущено к использованию, имеет сертификаты и нотификации.
- Роутеры Keenetic поддерживают современные классы Wi-Fi.
- Доступ в интернет с резервированием и балансировкой нагрузки.
- Широкие возможности вариантов подключения к сети Интернет.
- Масштабируемое Wi-Fi покрытие офиса или частного дома с бесшовным роумингом по стандартам 802.11k/r/v.
- Процессоры устройств подходят для задач шифрования трафика.



Характеристики устройств для программных модулей Netimd

№ п/п	Модель роутера Keenetic		Процессор(SoC)			Оперативная память,		Flash	Кол-во портов USB		Порты Ethernet				Wi-Fi		
								-									
	Название	Индекс KN-....	Название	Частота, МГц	Ко л- во яд ер	Размер, Мбайт	Тип DDR	Размер, Мбайт	2 .0	3.0	Ко л- в о	Скорость Мбит/с	S F P	Co mb o R J 45/ S F P	2,4ГГц, Мбит/ с	5ГГц, Мбит/ с	Класс
1	Peak	2710	MT7622B	1350	2	512	3	256	1	1	10	1000	1	0	800	1733	AC2600
2	Ultra SE	2510	EN7516GT	900	2	256	3	128	1	1	9	1000	0	0	800	1733	AC2600
3	Ultra	1810	MT7621A	880	2	256	3	128	1	1	5	1000	0	1	800	1733	AC2600
4	Giga	1010	MT7621A	880	2	256	3	128	1	1	5	1000	0	1	400	867	AC1300
5	Giga	1011	MT7621A	880	2	512	3	128	1	1	5	1000	0	1	574	1201	AX1800
6	Hopper	3810	EN7528DU	900	2	256	3	128	0	1	4	1000	0	0	574	1201	AX1800
7	Giant	2610	MT7621A	880	2	256	3	128	1	1	9	1000	0	1	400	867	AC1300
8	Hero 4G	2310	MT7621A	880	2	128	3	128	1	0	5	1000	0	0	400	867	AC1300
9	Giga SE	2410	EN7516GT	900	2	256	3	128	1	1	5	1000	0	0	400	867	AC1300
10	Viva	1910	MT7621A	880	2	128	3	128	2	0	5	1000	0	0	400	867	AC1300
11	Viva	1912	EN7528DU	900	2	256	3	128	1	0	4	1000	0	0	300	867	AC1200
12	Duo	2110	EN7513T	900	2	128	3	128	1	0	4	100	0	0	300	867	AC1200
13	Extra	1713	MT7628N	580	1	128	2	32	1	0	4	100	0	0	300	867	AC1200
14	4G	1212	MT7628N	575	1	128	2	32	1	0	4	100	0	0	300	-	N300
15	Omni	1410	MT7628N	575	1	128	2	32	1	0	5	100	0	0	300	-	N300
16	DSL	2010	EN7512U	700	2	128	2	128	1	0	4	100	0	0	300	-	N300



Спасибо за внимание!

Контактные данные:



Федоров С.И.



fedorov@imdtech.ru