Абсурдистанская Корпорация «Logos Corp»

Документация по официальному модулю МСТУ «Logos»:

«Cipher» (Сайфер)

LOGOS CORP

Издание: №1

Редакция печатных изданий инструкций Logos Corp

Специально для ознакомления

Продукт не подлежит свободной продаже!

2024 год

Оглавление

Введение....3
Основные протоколы и их свойства....5
Основные команды и их синтаксис....7

LOGOS CORP

Введение

Модуль Cipher (Сайфер) – представляет собой модуль для создания локальной зашифрованной сети между несколькими терминалами Logos. Цель данного модуля: Обеспечение защищенной передачи данных между терминалами. Защищенность достигается благодаря нескольким степеням шифрования:

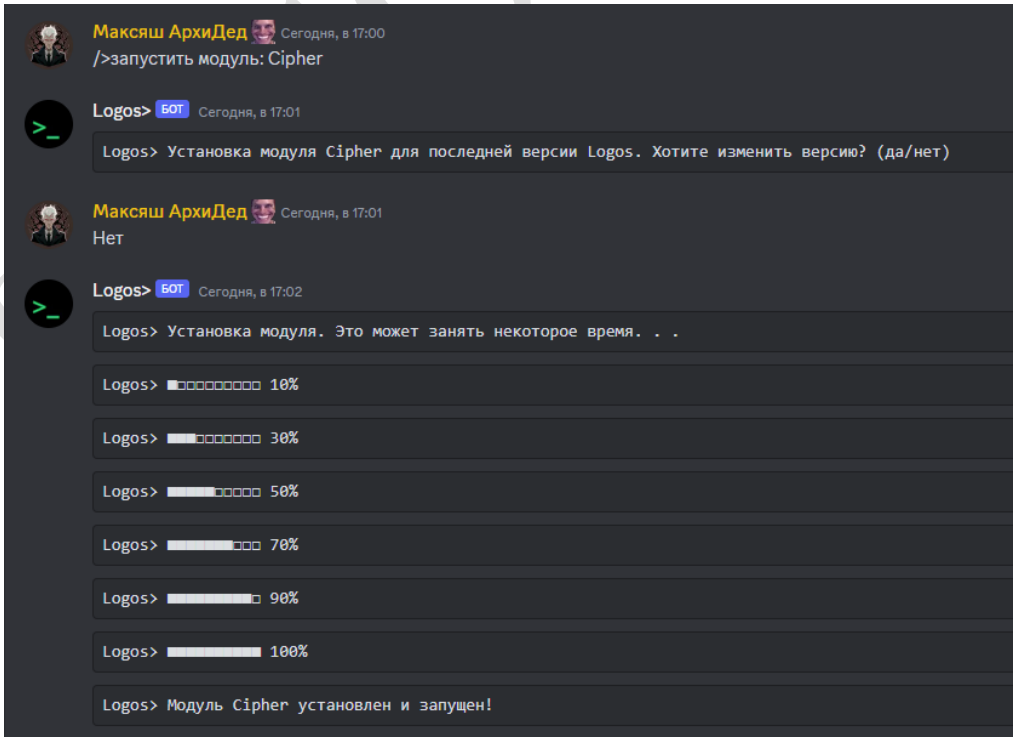
1. Как только данные были отправлены – они тут же шифруются в нечитабельный для человека вид. (1й уровень шифрования);

2. Затем, отправленным данным предстоит пройти не менее, чем через 2 узла дополнительного шифрования (УДШ). Каждый узел повторно шифрует данные (На выходе получаем минимум 3й уровень шифрования). На этом этапе скрываются метаданные, которые предотвращают утечку местоположения отправителя. Изначальный узел, с которого отправлены данные – практически невозможно опознать на данном этапе.

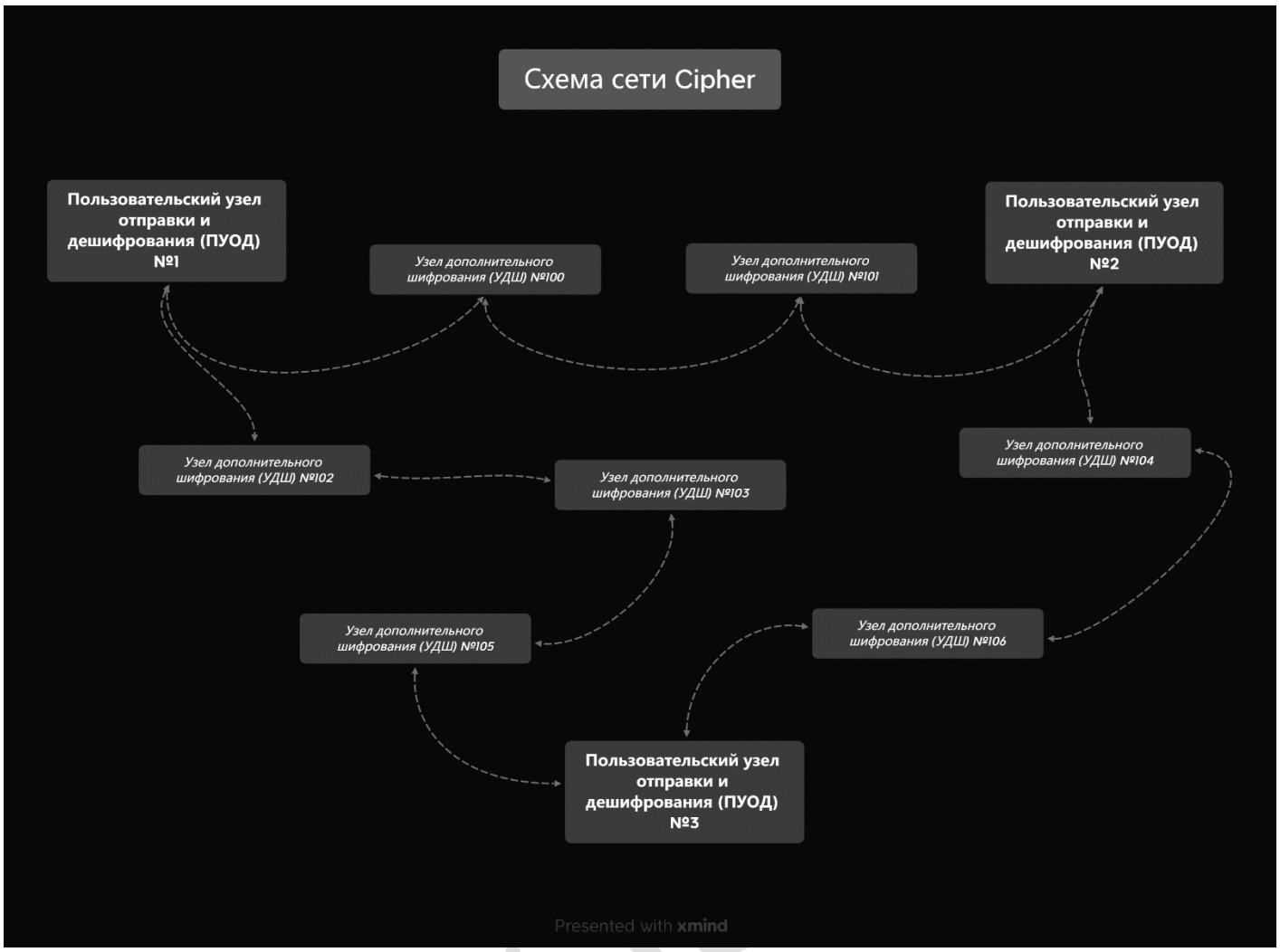
3. Данные приходят в точку назначения в зашифрованном виде. И только на этом этапе второй пользователь может дешифровать данные. (Притом, для того, чтобы можно было отправить данные и дешифровать их – необходимо, чтобы терминалы были соединены, т.е. оба пользователя должны подтвердить сопряжение).

Обязательное шифрование нельзя отключить будучи обычным пользователем.

Что касается установки модуля, то она максимально простая (как и установка других модулей). Вам просто нужно ввести команду **/>запустить модуль: Cipher** и дождаться установки и запуска модуля:



Образец того, что представляет из себя сеть Сайфер:



ПУОД также для простоты называют просто **Машинами**, т.е. это терминалы, которыми управляют люди (или в них были внедрены автономные протоколы), а УШД или просто **Узлы** – выступают исключительно в качестве шифровщиков.

Любой узел и любая машина имеют определенный адрес (явный и условный), который помогает им анонимно выполнять соединения друг с другом. **Явный адрес имеет вид: xxxx.z:n**, где:

xxxx – Номер машины или узла (обычно содержит 4 цифры, но может быть как короче, так и длиннее).

z – Номер локальной сети, где располагается узел или машина.

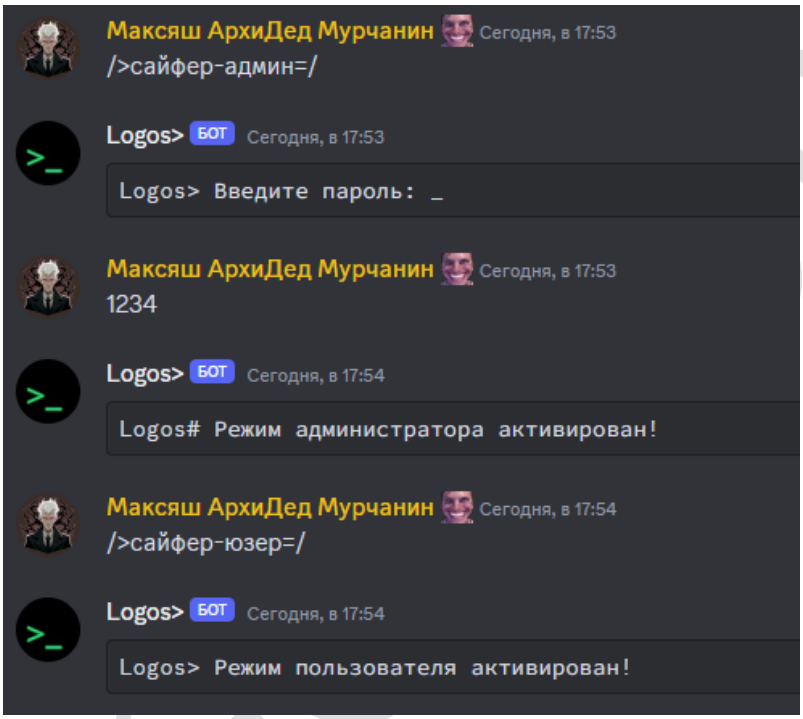
n – Количество портов у машины или узла. Однако, у УШД обычно нет ограничений на количество портов. Число портов отражает то, сколько машин может одновременно связаться с текущим узлом/машиной.

Например: 1984.5:3 – Номер узла/машина: 1984, номер локальной сети: 5, Количество портов: 3.

Условный адрес: xxx.xxx.xxx.z:n

Основные протоколы и их свойства

Машинами (терминалами) люди управляют вручную, т.е. самостоятельно настраивают соединения, самостоятельно передают данные и т.д. Однако, процесс передачи данных (а в особых случаях процесс соединения) можно автоматизировать. Для автоматизации разных процессов модуля, применяются протоколы. Чтобы установить тот или иной протокол – необходимо перейти в режим администратора командой **/>сайфер-админ=/**. После этого, Логос запросит пароль от машины. Чтобы вернуться в обычный режим, используйте команду **/>сайфер-юзер=/**



Рассмотрим некоторые из протоколов:

1) Протокол Logos-Iter (LI) (Метод маршрута) – протокол, который передает данные лишь выбранным машинам, игнорируя остальные даже при соединении с ними. Т.е. когда в машину с протоколом LI попадают данные – устройство автоматически пересылает их другим устройствам, которые находятся в путевой таблице. Путевая таблица содержит адреса всех терминалов, которым могут быть переданы данные. Для настройки путевой таблице используется команда />conf-LI=/

2) Протокол Logos-Civitas (LC) (Метод общности) – более простой протокол, суть которого: передача получаемых данных всем машинам, с которыми в данный момент имеется связь. Кроме того, данный протокол можно модернизировать дополнительным параметром: Logos-Ipso-Nexu (LIN). Его суть: отправка эхо-запроса на соединение ко всем терминалам поблизости, если то или иное устройство одобряет связь – Ваша машина будет автоматически пересылать данные по принципу LC. С помощью команды />conf-LC-LIN=/ можно изменять текст эхо-запроса. По умолчанию он имеет примерно следующий вид: «Привет! У меня есть важное сообщение для тебя!»

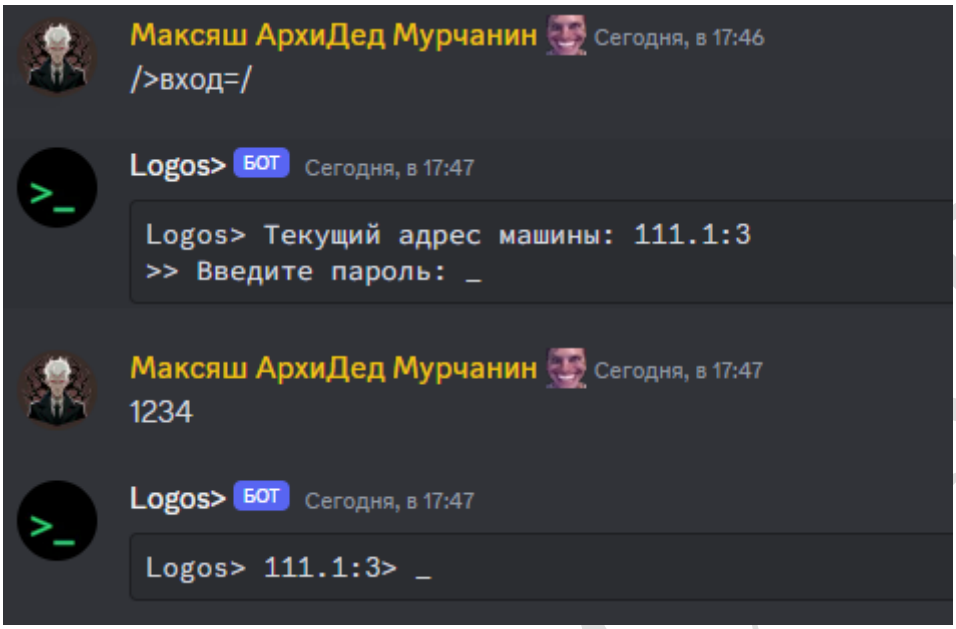
3) Протокол Logos-Subord (LS) (Метод подчинения) – протокол, который работает в пассивном режиме, ожидая, когда к машине попытается подключиться кто-либо для получения данных. Когда кто-то делает запрос на связь – LS-машина отправляет сообщение, в котором запрашивает пароль для соединения. Если пароль верный – машина автоматические пересылает запрашиваемому устройству все накопленные пакеты данных. Если пароль окажется трижды неверным – LS-машина заблокирует входящий трафик от этой машины. Кроме того, командой />conf-LS=/ можно изменять некоторые параметры машины, такие как пароль, сообщение с требованием ввода пароля, количество допустимых попыток.

4) Протокол AExm – протокол, который позволяет создавать самоуничтожающиеся файлы и отправлять их. Когда файл будет получен и просмотрен получателем – спустя определенный срок файл будет уничтожен. Срок жизни файла редактируется командой />conf-AExm=/

LOGOS CORP

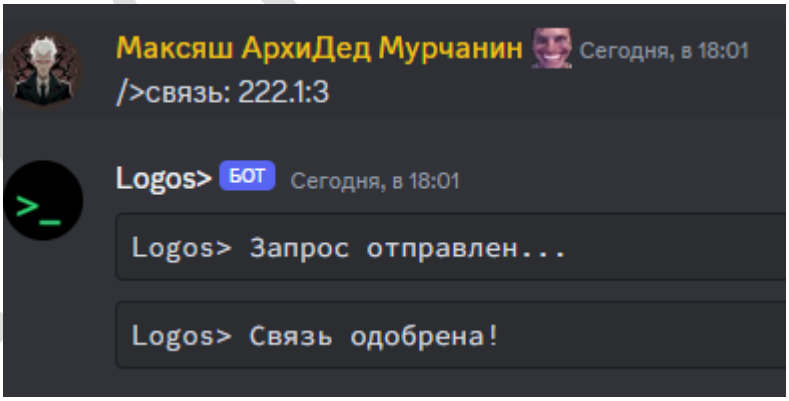
Основные команды и их синтаксис

1) **/>вход=/** Применяется для сетевого входа в свою машину



2) **/>выход=/** Применяется для завершения сетевого сеанса

3) **/>связь: адрес машины** Применяется для запроса на установление соединения с другой машиной. Адрес машины может быть как явным (если Вы его знаете) (пример ниже), либо условным (разбирается в пункте 7).



4) **/>разрыв: адрес машины** Применяется для принудительного разрыва соединения с машиной.

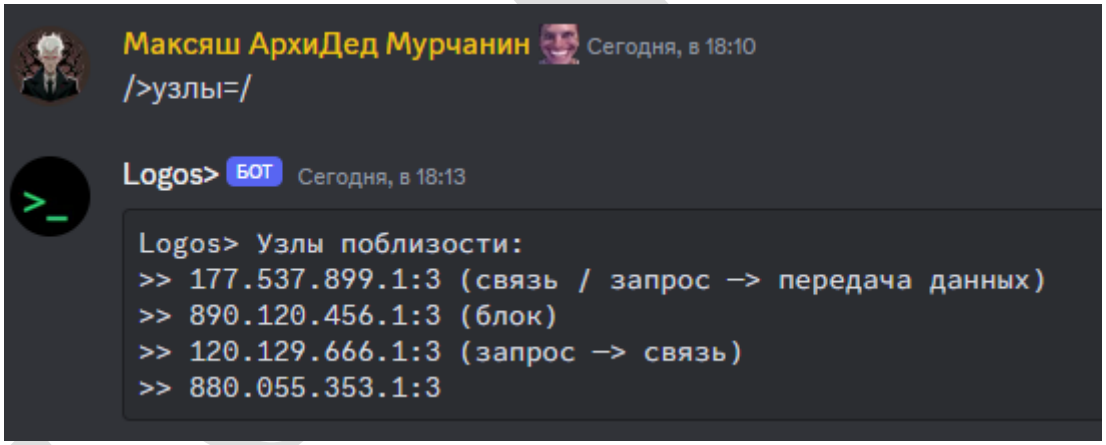
5) **/>блок: адрес машины** Применяется для блокировки трафика от машины. Это значит, что машина не сможет отправлять данные Вам.

6) **/>разблок: адрес машины** Применяется для снятия блокировки трафика с машины, предоставляя ей доступ отправлять Вам данные.

7) **/>узлы=/** Отображает все терминалы поблизости. Обратите внимание! Здесь не будет отображен Ваш узел, здесь не будут отображены УДШ, а все адреса терминалов являются условными, т.к. отображаемый адрес шифруется в целях безопасности (P.S. Ваш адрес тоже шифруется для других терминалов, но не для Вас самих).

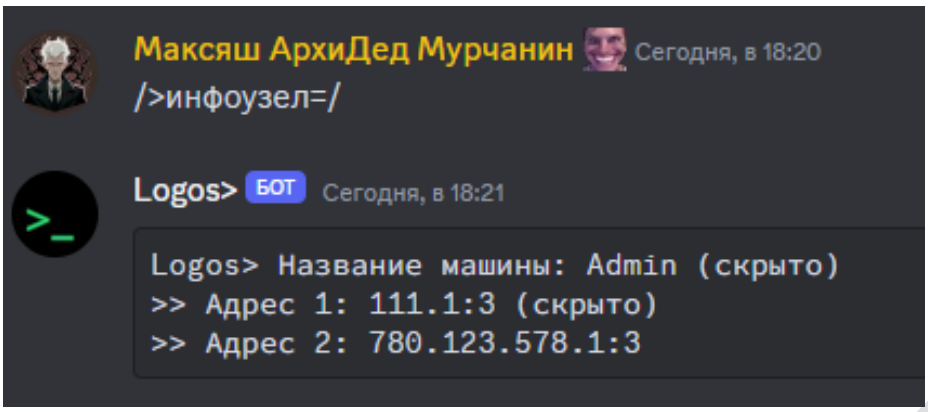
На изображении ниже мы видим зашифрованные адреса машин, но можем отследить состояния: связь – установлено соединение, запрос>передача данных – от Вашей машины исходит запрос на передачу данных или данные в процессе передачи, запрос>связь – от Вашей машины поступает запрос на соединение.

Заметьте! Установленное соединение не всегда дает возможность свободно отправлять файлы и данные. Банально, но устройстве Вашего товарища может стоять протокол, который принимает данные только в том случае, если Вы введены правильный пароль.

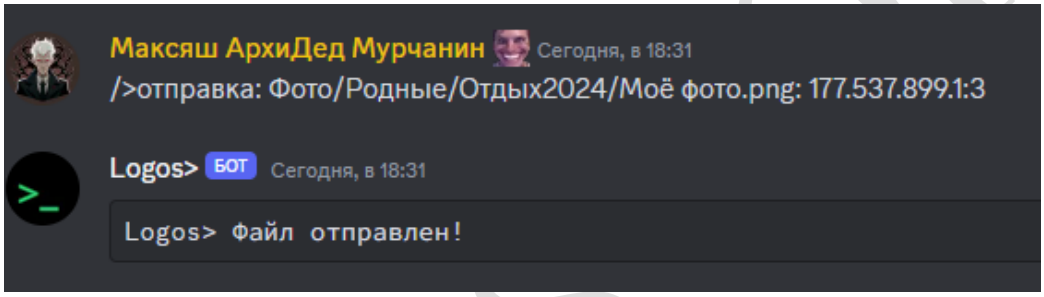


8) **/>ифноузел=/** Применяется, когда Вам нужно просмотреть данные о своем узле. Здесь уже отображается не только явный адрес, но и условный. А используя команду **/>настройки: сайфер: главные** Вы можете менять некоторые параметры, а именно: включить/выключить отображение Вашего явного адреса (команда **/>скрыть: адрес** или **/>показать: адрес**), включить/выключить отображение Вашего имени, т.е. имени машины (команда **/>скрыть: имя** или **/>показать: имя**).

Заметьте! Отображаемый адрес и имя будут видны всем устройствам поблизости. В целях безопасности рекомендуется оставить оба параметра по умолчанию выключенными.



9) **/>отправка**: **путь к файлу и имя файла: адрес машины** Позволяет отправлять файлы на другие машины. P.S. По умолчанию все входящие файлы будут храниться в папке **сайфер/файлы**



Обратите внимание, что Логос позволяет писать путь к файлу двумя способами: **Фото/Родные/Отдых2024…** и **Фото>Родные>Отдых2024…** Однако, комбинировать эти две записи нельзя!

10) **/>настройки: сайфер: пароль: старый пароль: новый пароль** Позволяет задать новый пароль сетевого терминала. Однако, для этого нужно войти в режим администратора!

11) **/>доступ: полный или просмотр: адрес машины** Позволяет поделиться доступом к своему терминалу с другой машиной поблизости. Выбрав параметр «полный» - подключенное устройство сможет вносить изменения в сетевую часть Вашего терминала. Выбрав «просмотр» - устройство сможет только просматривать Ваши действия и открывать для просмотра другие сетевые папки и файлы.

Кроме того, можно сделать определенную папку или файл сетевым. Для этого нужно ввести **/>доступ: полный или просмотр: название файла или папки**

Система прав работает аналогично той, которой придерживаются устройства. Только теперь выбранная папка или файл будут отображаться у всех устройств, которые имеют полный уровень доступа или могут просматривать файлы.

LOGOS RP

Заметьте! Права, выданные файлам и папкам будут в приоритете. Это значит, что, например, если папка имеет атрибут «просмотр», то даже машина с доступом «полный» не сможет вносить изменения в папке.

Права можно сбросить командой:

/>доступ: сброс (Глобально сбрасывает права для машин и файлов/папок)

/>доступ: сброс: адрес машины (Сброс прав для конкретной машины)

/>доступ: сброс: путь и имя к файлу или папке (Сброс прав для конкретного файла или папки)

/>доступ: сброс: узлы (Сбрасывает права для всех машин)

/>доступ: сброс: папки или файлы (Сбрасывает права либо для всех папок, либо для всех файлов)

Чтобы папка или файл отображались всем устройствам поблизости не смотря на их права – введите команду **/>настройки: сайфер: доступ: полный или просмотр: путь к файлу или папке**

12) **/>протокол: название протокола: адрес Вашей машины: пароль** Позволяет подключить необходимый протокол. Заметьте, что для выполнения этой команды Вам нужно войти в режим администратора.

Подключив протокол AExm – все отправленные Вами файлы будут шифроваться по методу AExm и будут содержать в названии **AExm_Имя файла.расширение** (Например: AExm_Важный файл.txt)

Если Вы хотите применить протокол только на отдельный файл, то в названии файла укажите название протокола и поставьте нижнее подчеркивание: **AExm_**Имя файла

Помните, что даже для изменения имени файла на имя с префиксом протокола – нужны права администратора.

LOGOS CORP