

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**





**NETWORK PROTECTION SOLUTIONS** — универсальный шлюз безопасности, предназначенный для эффективной защиты внутренней сети от киберугроз. Разработан компаниями AVTECH и Смарт-Софт, работающих на рынках Узбекистана и России несколько десятков лет.

Основные функции модели:

- контроль и фильтрация интернет-трафика (межсетевое экранирование);
- управление доступом сотрудников и клиентов к сети предприятия;
- предотвращение и выявление хакерских атак;
- защита внутренней сети от компьютерных вирусов и вредоносных программ;
- организация защищенного соединения между удаленными филиалами предприятия.

Все функции устройства представлены в онлайн документации на сайте [NPSAV.uz](https://npsav.uz)  
<https://npsav.uz/support/>

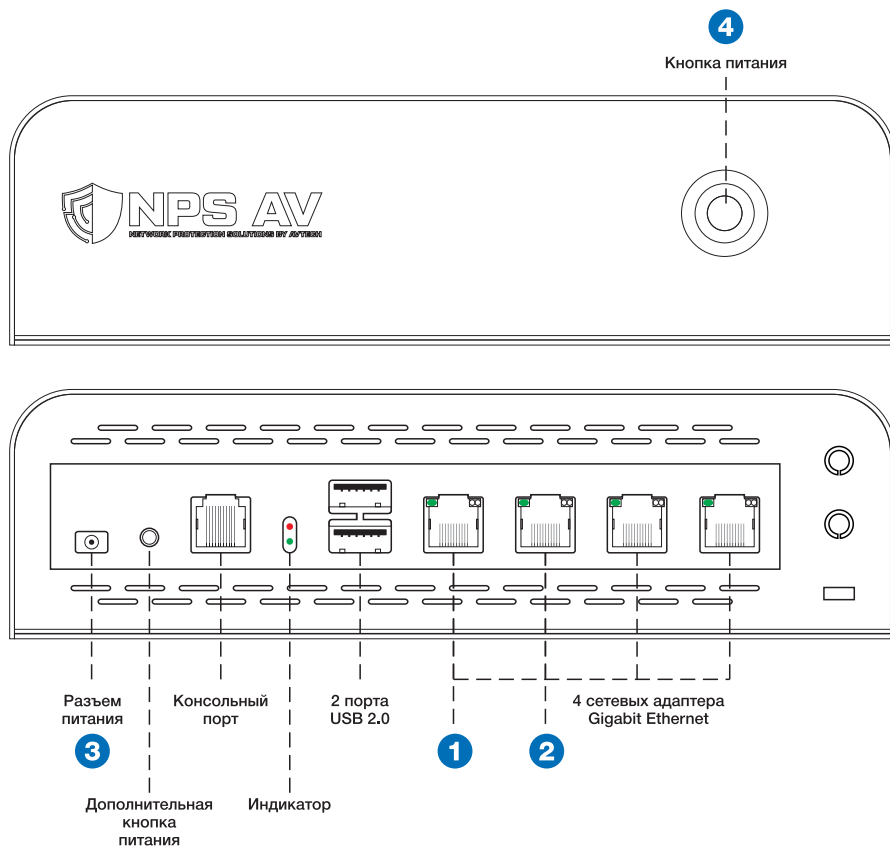


# СОДЕРЖАНИЕ

Внешний вид и подключение .....	3
Базовая настройка .....	6
Технические характеристики .....	16
Онлайн-инструкция и служба поддержки .....	22
О разработчике .....	23
Торговые марки .....	24

# ВНЕШНИЙ ВИД И ПОДКЛЮЧЕНИЕ

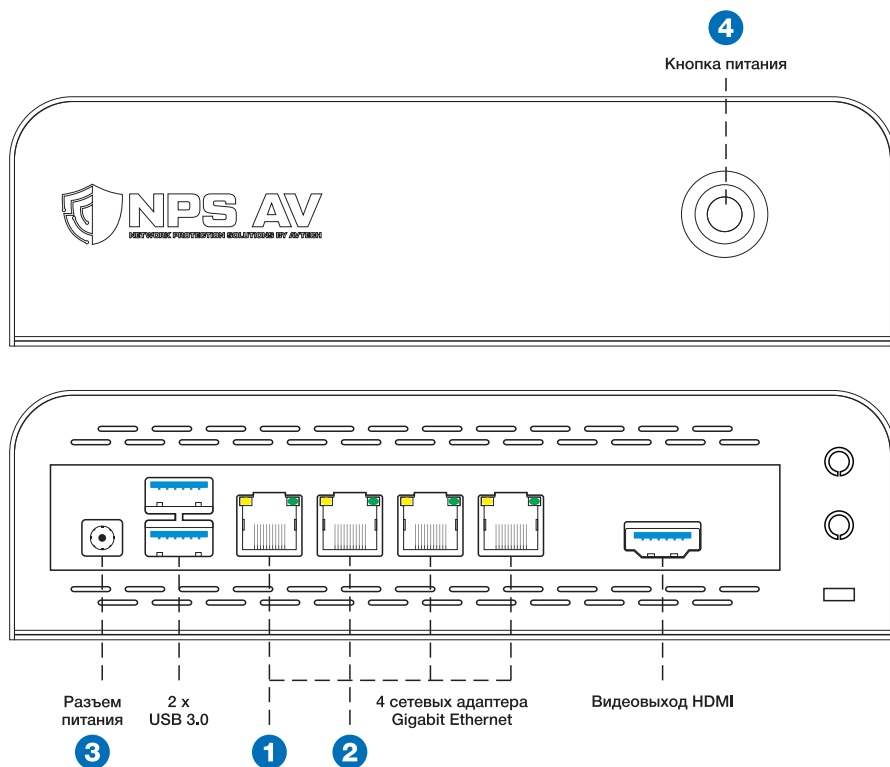
## AV-100



- 1 Подключите маршрутизатор локальной сети (роутер) к порту №1 на устройстве.
- 2 Подключите кабель интернет-провайдера к порту № 2.
- 3 Подключите питание.
- 4 Нажмите на кнопку питания.

Устройство готово к работе. Далее необходимо выполнить начальные настройки, активировать лицензию и обновить версию программного обеспечения.

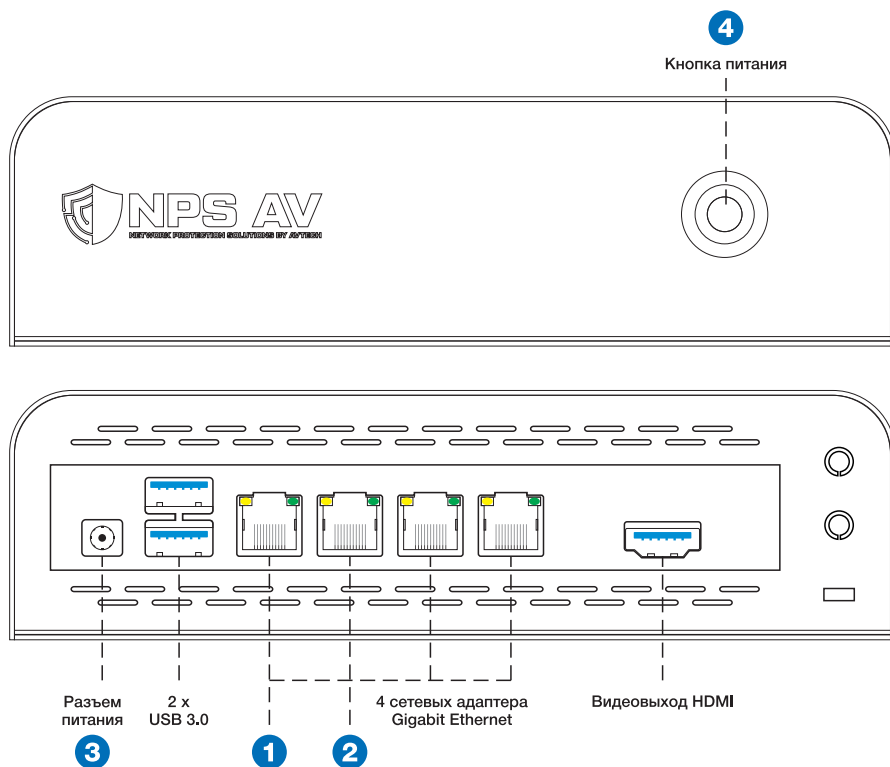
# AV-200



- 1 Подключите маршрутизатор локальной сети (роутер) к порту №1 на устройстве.
- 2 Подключите кабель интернет-провайдера к порту №2.
- 3 Подключите питание.
- 4 Нажмите на кнопку питания.

Устройство готово к работе. Далее необходимо выполнить начальные настройки, активировать лицензию и обновить версию программного обеспечения.

# AV-300



- 1 Подключите маршрутизатор локальной сети (роутер) к порту №1 на устройстве.
- 2 Подключите кабель интернет-провайдера к порту №2.
- 3 Подключите питание.
- 4 Нажмите на кнопку питания.

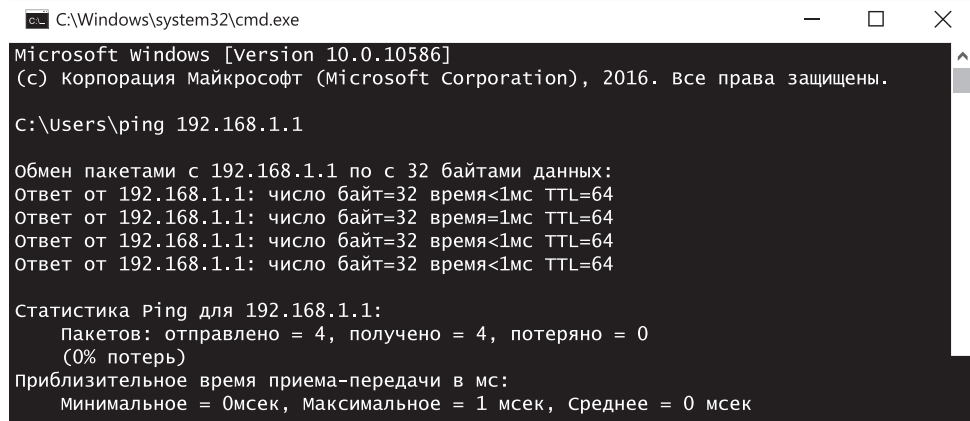
Устройство готово к работе. Далее необходимо выполнить начальные настройки, активировать лицензию и обновить версию программного обеспечения.

# БАЗОВАЯ НАСТРОЙКА

Наиболее удобный способ управления Network Protection Solutions AV-100, AV-200 и AV-300 — через интернет-браузер.

Наберите в адресной строке браузера **192.168.1.1**.

Для проверки соединения компьютера с Network Protection Solutions AV - выполните в командной строке команду ping (для операционной системы Windows нажать Win+R и набрать cmd): **ping 192.168.1.1**



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(с) Корпорация Майкрософт (Microsoft Corporation), 2016. Все права защищены.

C:\Users\ping > ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
```

При успешном соединении браузер предупредит о наличии небезопасного соединения.

Игнорируйте сообщение (на примере браузера Chrome: нажмите «Дополнительные» — «Перейти на сайт 192.168.1.1 (небезопасно)»). В случае успеха появится окно входа в Network Protection Solutions.

Используйте: логин - **root**, пароль - **npsav**.

## Шаг 1:

Запуск Мастера начальной настройки: раздел «Система» -> «Мастер».

В появившемся диалоге нажмите кнопку «Далее».

**В диалоге «Система: Мастер: Основная информация»** в разделе «Основная информация» можно изменить имя хоста (необязательно), указать домен (при использовании Microsoft AD), выбрать язык интерфейса

Задайте DNS-серверы: первичный — обязательно, например DNS провайдера, вторичный — если имеется. Если DNS провайдера неизвестен, укажите **DNS 8.8.8.8**.

Раздел «Unbound DNS» рассчитан только на опытных пользователей.



## ПРИМЕЧАНИЕ

Устройство поддерживает DNS от Яндекса (dns.yandex.ru):

- «Безопасный» 77.88.8.88 и 77.88.8.2 с антивирусом против мошеннических сайтов и вирусов;
- «Семейный» 77.88.8.7 и 77.88.8.3 с дополнительной функцией блокировки сайтов «для взрослых»

## Система: Мастер: Мастер настройки NPS

Этот мастер проведёт вас через начальную настройку Мастера можно прервать в любой момент нажатием на логотип вверху экрана.

Далее

## Система: Мастер: Основная информация

### Основная информация

Имя хоста:

Домен:

Язык:

Первичный DNS сервер:

Вторичный DNS сервер:

Переопределять DNS :  Разрешить переопределение DNS серверов настройками DHCP/PPP на WAN

### Unbound DNS

Включить распознаватель:

Включить поддержку DNSSEC:

Данные только DNSSEC:

Далее

В диалоге **«Система: Мастер: Настройка времени»** в поле **«Имя сервера времени»** можно задать доменное имя сервера синхронизации времени (желательно) или использовать значение по умолчанию (отображение времени будет менее точным).

### Система: Мастер: Настройка времени

Имя сервера времени:

Укажите полное имя сервера времени.

Часовой пояс:

Далее

В диалоге **«Система: Мастер: Конфигурация WAN-интерфейса»** настройте интерфейс связи с провайдером интернета (WAN-интерфейс). Для этого необходимо установить тип взаимодействия, предоставляемый провайдером Интернета. Самый популярный тип, предоставляемый провайдером — DHCP. Данный тип установлен по умолчанию. В этом случае IP-адрес назначается автоматически внешним DHCP-сервером.

Все остальные типы связи рекомендованы для опытных пользователей.

Тип взаимодействия Static (IP-адрес назначается пользователем, им же назначаются обязательные параметры: префикс подсети, IP-адрес маршрутизатора по умолчанию), PPPoE (взаимодействие на уровне протокола канального уровня PPP, здесь можно указать параметры аутентификации на сервисе PPPoE и название сервиса), PPTP (защищенное соединение типа «точка — точка» с использованием туннельного протокола на уровне протокола IP, здесь можно задать параметры аутентификации, локальный IP-адрес для устройства, а также IP-адрес сервера PPTP).

Настройка параметров общей конфигурации - собственный MAC-адрес для WAN-интерфейса, собственное значение MTU (максимальная длина кадра) и MSS (максимальная длина сегмента) - рекомендована для опытных пользователей.



#### ПРИМЕЧАНИЕ

Если провайдер предоставляет IP-адреса из диапазона частных сетей, в настройках WAN-интерфейса необходимо снять галочку с пункта «Блокировать частные сети».

## Система: Мастер: Конфигурация WAN интерфейса

Тип конфигурации IPv4:

### Общая конфигурация

MAC адрес:

Это поле используется для изменения ("спуфинг") MAC адрес WAN интерфейса (может потребоваться для некоторых кабельных подключений). Введите MAC адрес в следующем формате: xx:xx:xx:xx:xx:xx или оставьте пустым.

Максимальный размер кадра:

Укажите MTU WAN интерфейса. Если вы оставите это поле пустым, MTU будет равно 1492 байт для PPPoE и 1500 байт для всех остальных типов подключений.

Максимальный размер сегмента:

Если вы введёте значение в это поле, то MSS clamping для TCP соединений будет равно введённому значению минус 40 (размер заголовка TCP/IP). Если вы оставите это поле пустым, MSS будет равно 1492 байт для PPPoE и 1500 байт для всех остальных типов соединений. Это должно подходить для значений MTU в большинстве случаев.

### Статическая конфигурация IP

IP-адрес:

Основной шлюз:

### Конфигурация DHCP-клиента

Имя хоста для DHCP:

Значение этого поля отправляется в качестве идентификатора DHCP-клиента и имени хоста при запросе аренды адреса. Некоторые поставщики услуги Интернет могут потребовать это значение (для идентификации клиента)

## Конфигурация PPPoE

Имя пользователя PPPoE:

Пароль PPPoE:

Имя сервиса PPPoE:

PPPoE соединение по требованию:  Включить режим «Соединение по запросу»

Это опция заставляет интерфейс работать в режиме соединения по требованию, позволяя Вам иметь виртуальное постоянное соединение. Интерфейс настроен, но реальное соединение отложено до того момента, когда будет обнаружен исходящий трафик.

Таймаут отключения PPPoE:

Если в течение указанного количества секунд не передается ни одного квалифицирующего исходящего пакета, соединение прерывается. Время простоя, равное нулю, отключает эту функцию.

## Конфигурация PPTP

Имя пользователя PPTP:

Пароль PPTP:

Локальный IP адрес PPTP:

32

IP адрес сервера PPTP:

Соединение PPTP по требованию:  Включить режим «Соединение по запросу»

Это опция заставляет интерфейс работать в режиме соединения по требованию, позволяя Вам иметь виртуальное постоянное соединение. Интерфейс настроен, но реальное соединение отложено до того момента, когда будет обнаружен исходящий трафик.

Таймаут отключения PPTP:

Если в течение указанного количества секунд не передается ни одного квалифицирующего исходящего пакета, соединение прерывается. Время простоя, равное нулю, отключает эту функцию.

## RFC1918 сети

Блокировать частные сети RFC1918:  Блокировка доступа частных сетей из WAN

Если этот параметр задан, он блокирует трафик с IP-адресов, зарезервированных для частных сетей в соответствии с RFC 1918 (10/8, 172.16/12, 192.168/16), а также адреса loopback (127/8) и адреса Nat Carrier-grade (100.64/10). Этот параметр должен быть установлен только для интерфейсов WAN, использующих общедоступное IP-адресное пространство.

## Блокировать bogon сети

Блокировать bogon сети:  Блокировка не Интернет маршрутизируемых сетей из WAN

Этот параметр блокирует трафик от IP-адресов, которые зарезервированы (но не RFC 1918) или еще не присвоены IANA.

Далее

В диалоге **«Система: Мастер: Конфигурация LAN-интерфейса»** пользователь может изменить параметры интерфейса LAN, IP-адрес и маску подсети. Рекомендуется оставить параметры по умолчанию. Данные параметры необходимо изменять только опытным пользователям.

## Система: Мастер: Конфигурация LAN интерфейса

IP адреса LAN:

(можете оставить пустым)

Маска подсети:

Далее

В диалоге «**Система: Мастер: Ввод пароля администратора**» пользователь может сменить пароль пользователя root.

### Система: Мастер: Ввод пароля администратора

Пароль администратора:

(оставьте пустым для сохранения текущего значения)

Подтверждение пароля администратора:

Далее

### ПРИМЕЧАНИЕ

В целях безопасности исходный пароль необходимо заменить на собственный.

### Система: Мастер: Перезагрузить конфигурацию

Нажмите 'Перезагрузить', чтобы применить изменения.

Перезагрузить

После перезагрузки системы будет открыт доступ к сети Интернет и репозиторию плагинов Network Protection Solutions

### Шаг 2:

Установка лицензии: «**Главное меню**» -> «**Сводка**» -> «**Лицензия**».

Если лицензия в форме хеш-последовательности (длинная строка цифр и букв), введите ее в поле «**Лицензионный ключ**» и нажмите «**Активировать лицензию**».

Если лицензия в виде текстового файла, нажмите «**Импортировать лицензию**», выберите файл и нажмите «**Активировать лицензию**».

После того как лицензия активирована, она отображается в списке лицензий.

## Сводка: Лицензия

Модуль	Истекает	Организация	Лицензия	Примечание
CORE	2019-09-21	Smart-Soft Ltd	775e17a3ccf5e73226901d8b10e92f0b	Лицензия недействительна для этого устройства
CMS_MASTER	Просрочена	Smart-Soft Ltd	3658d61e0a3d9824200e082ba02a9783	Лицензия недействительна для этого устройства
NETPOLICE	Просрочена	Smart-Soft Ltd	79a074f8fb7a309d735fa93ca203d100	Сертификат не соответствует секретному ключу

Показаны с 1 по 3 из 3 записей

## Получение лицензии

 Лицензионный ключ

Активировать лицензию

Экспортировать лицензию

Импортировать лицензию

## Шаг 3:

Обновление программного обеспечения:

«Главное меню» -> «Система» -> «Прошивка» -> «Проверить наличие обновлений».

Если будет обнаружена более новая версия ПО, нажмите «Обновить сейчас», дождитесь завершения обновления и перезапуска системы.

## Система: Прошивка

Доступно обновление 1, общий размер загружаемых файлов 5.0MiB.

Проверить наличие обновлений

Обновить сейчас

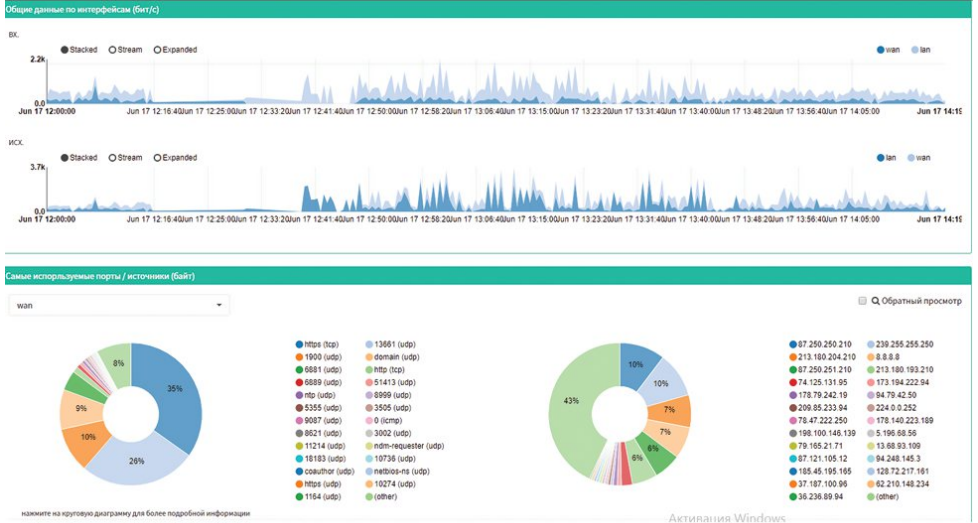
Обновления	Плагины	Пакеты	Настройки
Имя пакета	Текущая версия	Новая версия	Необходимое действие
ting	1.4.1.rcL_22	1.4.1.rcL_25	обновить

Базовые настройки завершены. В устройстве активированы основные функции.

Функции в базовых настройках:

- DHCP сервер - выделение IP адресов устройствам в локальной сети;
- межсетевой экран - предоставление доступа в сеть Интернет на основании правил межсетевого экранирования по умолчанию.

Для просмотра статистики сетевого трафика необходимо включить функцию Netflow:  
«Главное меню» -> «Создание отчетов» -> «NetFlow»



Отчет по сетевой статистике доступен в разделе «Анализ» и содержит данные о том, какой компьютер на какой адрес обращался, по какому порту/сервису и сколько данных было передано по каждому взаимодействию.

Также система формирует отчеты с распределением трафика по портам назначения, сетевым службам, IP-адресам назначения и т.п.

Для выгрузки данных в разделе «Анализ» предусмотрена вкладка «Экс- порт».

Для продвинутого использования устройства необходимо произвести дополнительные настройки Network Protection Solutions.



Воспользуйтесь инструкциями по настройке на сайте NPSAV.uz  
<https://npsav.uz/docs-category/soderzhanie/>

или видеуроками:  
[https://www.smart-soft.ru/support/documentation/video\\_ting/](https://www.smart-soft.ru/support/documentation/video_ting/)

Функции, требующие дополнительной настройки и установки плагинов:

- Управление доступом сотрудников и клиентов к сети Интернет как для незащищенного, так и защищенного соединения.
- Для настройки перейдите в раздел **«Межсетевой экран и NAT»**:  
<https://npsav.uz/docs/logika-raboty/>  
и в разделе «Веб-прокси» руководства пользователя на сайте NPSAV.uz:  
<https://npsav.uz/docs/bazovye-nastrojki-veb-proksi/>
- Предотвращение и выявление хакерских атак - сканирование сетевого трафика на предмет выявления вредоносных сигнатур.
- Для настройки перейдите в раздел **«Система обнаружения / предотвращения вторжений»** руководства пользователя на сайте NPSAV.uz:  
<https://npsav.uz/docs/ids-ips/>.
- Защита внутренней сети от компьютерных вирусов и вредоносных программ.
- Организация защищенного соединения между удаленными филиалами предприятия - VPN каналы.

Для настройки перейдите в раздел «VPN» руководства пользователя на сайте NPSAV.uz:  
<https://npsav.uz/docs/vpn/>

# ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

## NETWORK PROTECTION SOLUTIONS AV-100

Класс решения	UTM
Платформа	OPNsense
Межсетевой экран	есть
Система обнаружения и предотвращения вторжений	основана на коде и сигнатурах Suricata, а также поддерживает правила ET Open, интегрирована сSSL Blacklist (SSLBL) и трекером Feodo.
Организация шифрованных VPN-каналов	Между филиалами, партнерскими организациями, удаленными сотрудниками и центральным офисом. Благодаря интеграции с СКЗИ «МагПро Криптопакет» вы сможете организовывать шифрованные по ГОСТ VPN-каналы связи. Это важно, если вы работаете с государственными учреждениями
Двухфакторная аутентификация пользователей	есть
Функция прокси-сервера	есть
Правила доступа	разные для разных категорий сотрудников: разрешенные или запрещенные сайты («черные» и «белые» списки) для разных категорий пользователей автоматическая блокировка нежелательного или вредоносного контента блокировка приложений правилами глубокой пакетной инспекции
Дополнительные модули	модуль антивирусной защиты Anti-Virus powered by Kaspersky обеспечивает проверку трафика (HTTP(S) и FTP), проходящего через прокси-сервер и почтовый шлюз программы Network Protection Solutions; фильтр контента NetPolice фильтрует сайты по категориям и их содержанию, не позволяет получить доступ к определенным сайтам или услугам сети Интернет (например, к вредному и опасному для детей и подростков контенту).
	Аппаратные характеристики
Модель	NPS AV-100
Процессор	D525
Сеть	4 x 1 GbE
Порты GbE RJ45 [10/100/1000 Мбит/с]	4 GBE
Порты USB	2 USB 2.0
Консольный порт	-

Устройство хранения данных	120 GB
Оперативная память	4 GB
CPU / ядро	1,8 GHz quad Core
Виртуальные интерфейсы	4093
	Размеры
Высота/ширина/длина (мм)	56/192/194
Вес (кг)	0,45
	Рабочая среда
Питание	19 V
Максимальный ток	1,5 A
Потребление электроэнергии (усредненное)	80 W
Рабочая температура	0 до +45 °C
Температура хранения	-20 до +70 °C
Влажность	10-90% без конденсации

# NETWORK PROTECTION SOLUTIONS AV-200

Класс решения	UTM
Платформа	OPNsense
Межсетевой экран	есть
Система обнаружения и предотвращения вторжений	основана на коде и сигнатурах Suricata, а также поддерживает правила ET Open, интегрирована cSSL Blacklist (SSLBL) и трекером Feodo.
Организация шифрованных VPN-каналов	Между филиалами, партнерскими организациями, удаленными сотрудниками и центральным офисом. Благодаря интеграции с СКЗИ «МагПро Криптопакет» вы сможете организовывать шифрованные по ГОСТ VPN-каналы связи. Это важно, если вы работаете с государственными учреждениями
Двухфакторная аутентификация пользователей	есть
Функция прокси-сервера	есть
Правила доступа	<p>разные для разных категорий сотрудников:</p> <p>разрешенные или запрещенные сайты («черные» и «белые» списки) для разных категорий пользователей</p> <p>автоматическая блокировка нежелательного или вредоносного контента</p> <p>блокировка приложений правилами глубокой пакетной инспекции</p>
Дополнительные модули	<p>модуль антивирусной защиты Anti-Virus powered by Kaspersky обеспечивает проверку трафика (HTTP(S) и FTP), проходящего через прокси-сервер и почтовый шлюз программы Network Protection Solutions;</p> <p>фильтр контента NetPolice фильтрует сайты по категориям и их содержанию, не позволяет получить доступ к определенным сайтам или услугам сети Интернет (например, к вредному и опасному для детей и подростков контенту).</p>
	Аппаратные характеристики
Модель	NPS AV-200
Максимальное число пользователей	200
Процессор	Intel Core i3
Сеть	4 x 1 GbE
Порты GbE RJ45 [10/100/1000 Мбит/с]	4 GBE
Порты USB	2 USB 3.0

Видеовыход	HDMI
Устройство хранения данных	120 GB
Оперативная память	8 GB
CPU / ядро	4 / 4
Виртуальные интерфейсы	4093
	Размеры
Высота/ширина/длина (мм)	55/193/195
Форм фактор	6 x 6» (152,4 x 152,4 мм)
Вес (кг)	0,45
	Рабочая среда
Питание	19 V
Максимальный ток	1,5 A
Потребление электроэнергии (усредненное)	80 W
Рабочая температура	0 до +45 °C
Температура хранения	-20 до +70 °C
Влажность	10-90% без конденсации

# NETWORK PROTECTION SOLUTIONS AV-300

Класс решения	UTM
Платформа	OPNsense
Межсетевой экран	есть
Система обнаружения и предотвращения вторжений	основана на коде и сигнатурах Suricata, а также поддерживает правила ET Open, интегрирована cSSL Blacklist (SSLBL) и трекером Feodo.
Организация шифрованных VPN-каналов	Между филиалами, партнерскими организациями, удаленными сотрудниками и центральным офисом. Благодаря интеграции с СКЗИ «МагПро Криптопакет» вы сможете организовывать шифрованные по ГОСТ VPN-каналы связи. Это важно, если вы работаете с государственными учреждениями
Двухфакторная аутентификация пользователей	есть
Функция прокси-сервера	есть
Правила доступа	<p>разные для разных категорий сотрудников:</p> <p>разрешенные или запрещенные сайты («черные» и «белые» списки) для разных категорий пользователей</p> <p>автоматическая блокировка нежелательного или вредоносного контента</p> <p>блокировка приложений правилами глубокой пакетной инспекции</p>
Дополнительные модули	<p>модуль антивирусной защиты Anti-Virus powered by Kaspersky обеспечивает проверку трафика (HTTP(S) и FTP), проходящего через прокси-сервер и почтовый шлюз программы Network Protection Solutions;</p> <p>фильтр контента NetPolice фильтрует сайты по категориям и их содержанию, не позволяет получить доступ к определенным сайтам или услугам сети Интернет (например, к вредному и опасному для детей и подростков контенту).</p>
	Аппаратные характеристики
Модель	NPS AV-300
Процессор	Intel Core i3
Сеть	4 x 1 GbE
Порты GbE RJ45 [10/100/1000 Мбит/с]	4 GbE
Порты USB	2 USB 3.0

Видеовыход	HDMI
Устройство хранения данных	120 GB
Оперативная память	8 GB
CPU / ядро	4 / 4
Виртуальные интерфейсы	4093
	Размеры
Высота/ширина/длина (мм)	55/193/195
Форм фактор	6 x 6» (152,4 x 152,4 мм)
Вес (кг)	0,45
	Рабочая среда
Питание	19 V
Максимальный ток	1,5 A
Потребление электроэнергии (усредненное)	80 W
Рабочая температура	0 до +45 °C
Температура хранения	-20 до +70 °C
Влажность	10-90% без конденсации

# ОНЛАЙН-ИНСТРУКЦИЯ И СЛУЖБА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

[npsav.uz/docs-category/soderzhanie/](https://npsav.uz/docs-category/soderzhanie/)

Если вы столкнулись с проблемой при работе или настройке устройства, обратитесь в службу технической поддержки.

 **+998 71 207 00 89**

 **info@npsav.uz**

УСЛУГА НАСТРОЙКИ  
NETWORK PROTECTION SOLUTIONS «ПОД КЛЮЧ»



Смарт-Софт оказывает услуги по настройке и конфигурированию Network Protection Solutions: наш специалист удаленно подключится к вашей сети, произведет установку решения и настройку его функций согласно вашим требованиям.

Для заказа услуги свяжитесь с нами.

 **+998 71 207 00 89**

 **info@npsav.uz**



## О РАЗРАБОТЧИКЕ

Компания AVTECH была основана в 2001 году и на сегодняшний день успешно работает и развивается на рынке Узбекистана. Деятельность компании направлена на развитие отрасли информационных технологий, в частности: производство и насыщение рынка компьютерами, компьютерными корпусами, источниками бесперебойного питания, а также другими периферийными устройствами.

Компания Смарт-Софт – ведущий российский разработчик комплексных систем защиты информации и управления доступом в интернет для бизнеса, госсектора, образовательных и медицинских учреждений, учреждений культуры – многофункционального межсетевого экрана и системы обнаружения (предотвращения) вторжений, универсального шлюза безопасности (UTM) и системы обнаружения (предотвращения) вторжений.

Собственные решения на основе уникальных программных алгоритмов полностью соответствуют требованиям российского законодательства в области защиты информации.

Решения компании Смарт-Софт входят в Единый реестр российских программ для электронных вычислительных машин и баз данных и защищают компьютерные сети Газпрома, Мегафона, Сбербанка, РЖД, Роснефти, а также тысяч других компаний крупного, среднего и малого бизнеса и государственных организаций.

За 17 лет работы Смарт-Софт сформировала партнерскую сеть, состоящую более чем из 2500 российских и международных компаний.

# ТОРГОВЫЕ МАРКИ

Изделие компании AVTECH GROUP и соответствующая документация защищены авторскими правами.

Логотипы NETWORK PROTECTION SOLUTIONS являются торговой маркой компании AVTECH GROUP.

Другие названия компаний, продуктов и служб, приведенные в данном документе и в других его публикациях, могут являться торговыми марками или знаками обслуживания соответствующих владельцев.

Все права защищены.

Названия или марки компаний, упомянутые в руководствах к компьютеру или в данном документе, не являются признаком того, что соответствующее программное или аппаратное обеспечение прилагается.





[www.npsav.uz](http://www.npsav.uz)