NSG–1000/GW

Коммуникационный шлюз (маршрутизатор)

hardware versions D525MW, D2500CC

Руководство пользователя

Москва 2016

СОДЕРЖАНИЕ

ВНИМАНИЕ Продукция компании непрерывно совершенствуется, в связи с чем возможны изменения отдельных аппаратных и программных характеристик по сравнению с настоящим описанием.

ВНИМАНИЕ При получении устройства необходимо **ПРОВЕРИТЬ** комплектацию (см. последнюю страницу обложки). Отсутствие паспорта изделия со штампом ОТК и отметкой организации-продавца является основанием для отказа в гарантийном обслуживании и технической поддержке со стороны ООО «Эн-Эс-Джи».

Замечания и комментарии по документации NSG принимаются по адресу: doc@nsg.net.ru.

1. Общие сведения об устройстве

1.1. Назначение устройства

NSG–1000/GW — высокопроизводительный коммуникационный шлюз, предназначенный для использования в корпоративных сетях и сетях поставщиков услуг. Устройство выполняет роль центрального сервера доступа и поддерживает широкий набор технологий туннелирования и VPN, в том числе:

— механизмы инкапсуляции 2 уровня (Virtual Private Dial-In Networking): PPTP, PPPoE, с централизованной аутентификацией пользователей и учетом потребления услуг по RADIUS и TACACS+.

— механизмы 3 уровня: IPsec (в т.ч. NAT Traversal, сертификаты X.509 и др.), GRE (в т.ч. Cisco-совместимый механизм *keepalive*), IPv4-over-IPv6* и IPv6-over-IPv4*

— стандартные механизмы 4 уровня: STunnel, OpenVPN*

— фирменную технологию NSG ***ui*TCP** — VPN 4 уровня с множественным резервированием каналов связи, поддержанием бесперебойных сеансов работы прикладного ПО и гарантированной доставкой данных.

Максимальное количество туннелей всех вышеперечисленных типов программного не ограничено и определяется только средним объёмом трафика по одному туннелю и суммарной произволительностью устройства.

NSG–1000/GW также обладает всеми функциями IP-маршрутизатора общего назначения и может применяться в качестве такового.

Устройство работает под управлением программного обеспечения NSG Linux 2.0, поддерживающего современные технологии построения сетей IP и VPN. Все программные возможности, за исключением фирменных технологий NSG, реализованы в соответствии с действующими стандартами и спецификациями и совместимы с оборудованием других производителей. Использование NSG Linux описано в документе: *Мультипротокольные маршрутизаторы NSG. Программное обеспечение NSG Linux 2.0. Руководство пользователя.*

Полный перечень поддерживаемых функциональных возможностей и соответствующих им стандартов и спецификаций зависит от версии программного обеспечения и приведен в отдельном документе.

Установка новых версий программного обеспечения может производиться заказчиком по его усмотрению.

Все вышеперечисленные документы находятся на CD-ROM, входящем в комплектацию устройства, а также доступны на Web-сайте компании NSG в разделах:

http://www.nsg.ru/doc/
ftp://ftp.nsg.net.ru/pub/doc/

* На момент написания данного документа — в разработке.

NSG–1000/GW рассчитано на непрерывную круглосуточную работу в необслуживаемом режиме. Управление устройством может производиться локально или удалённо посредством HTTP/HTTPS, SNMP, SSH или Telnet, а также консольного порта.

Устройство имеет фиксированную аппаратную конфигурацию и выпускается в металлическом корпусе формата 19" высотой 1U с блоком питания переменного тока.

1.2. Технические характеристики устройства

Аппаратные характеристики (D525MW / D2500CC)

- Процессор Intel Atom D525 1,8 ГГц / D2500 1,86ГГц
- Оперативная память 4 ГБ
- Энергонезависимая память 2×512 МБ (опционально 512 МБ + HDD 320 ГБ)
- 2 порта Ethernet 10/100/1000Base–T, разъёмы RJ–45
- Порт RS–232 для передачи пользовательских данных (только *h/w ver.D2500CC*)
- Опции для *h/w ver.D2500CC**:
  - — 3-й порт Ethernet 10/100/1000Base–T, разъём RJ–45
  - — интерфейс Wi-Fi IEEE 802.11 b/g/n
  - — дополнительно 2 порта RS–232
- Консольный порт
- 6 портов USB

Физические характеристики

- Габариты: 450×403×45 мм (ш×г×в, без учёта выступающих частей)
- Масса (без сменных интерфейсных модулей): 5,5 кг
- Электропитание: ~115–230 В, макс. 100 Вт
- Условия эксплуатации: температура +5…+50°C
  относительная влажность 10–85%

Поддержка внешних устройств USB

- Generic Storage (Flash, HDD)
- WiMAX модемы: Samsung SWC–U200
- Принтеры: любые с поддержкой HP JetDirect

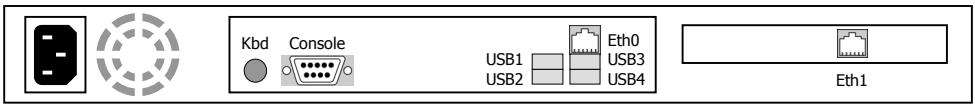
* Опции устанавливаются в заводских условиях. Одновременно возможна установка только одной опции.

2. Внешний вид устройства

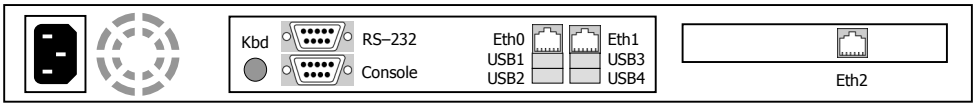
На передней панели устройства расположены следующие органы управления:

POWER	Индикатор наличия питания.
HDD	Индикатор активности Flash/HDD.
USB5, 6	Порты USB 5 и 6.
RESET	Кнопка для аппаратной перезагрузки устройства.
ON/OFF	Кнопка питания — не используется, устройство включено постоянно при наличии питания.

На задней панели устройства расположены следующие порты, в зависимости от модификации:



NSG–1000/GW *h/w ver.D525MW*



NSG–1000/GW *h/w ver.D2500CC*

Eth0, Eth1	Порты Gigabit Ethernet eth0, eth1.
Eth2	Порт Gigabit Ethernet eth2 (опционально).
USB1...4	Порты USB 1 … USB 4.
RS–232	Порт RS–232.
Console	Консольный порт для локального управления устройством.
Kbd	Разъём для подключения клавиатуры, используется при входе в сервисный режим работы устройства.

Колодка питания 220В.

Другие порты и разъёмы, имеющиеся на задней панели, в конфигурации устройства не задействованы.

3. Включение и подготовка к работе

3.1. Установка устройства

Для установки устройства в сеть необходимо:

1. Вскрыть упаковку устройства и убедиться в наличии полного комплекта документации и аксессуаров согласно п.6 данного руководства. Если фактическая комплектация не соответствует списку, обратитесь к поставщику, от которого получено данное устройство.
2. Установить устройство на предназначенное для него место на столе, в аппаратном шкафу или стойке.
3. Подключить порты Ethernet к локальным сетям Ethernet, либо непосредственно к устройствам, оборудованным сетевыми адаптерами Ethernet. Подключение порта к коммутатору локальной сети производится прямым кабелем; к ПК — перекрёстным кабелем. В большинстве конфигураций порт eth0 подключается к внутренней сети офиса, eth1 — к сети общего пользования.
4. Подключить консольный порт к COM-порту персонального компьютера при помощи кабеля CAV–V24/DB9/FC/A, входящего в комплектацию устройства, если первоначальное конфигурирование устройства предполагается производить через него.
5. Подключить устройство к источнику питания и включить выключатель питания, расположенный на задней панели.

3.2. Начальное конфигурирование устройства

Первоначальное конфигурирование устройства выполняется, как правило, через порт Fast Ethernet eth0 при помощи Web-броузера или клиента Telnet. В заводской конфигурации данный порт имеет адрес 192.168.1.1/24. Для работы с этим портом необходимо настроить на сетевом адаптере ПК любой другой адрес вида 192.168.1.*x* (*x* = 2 … 254) с маской 255.255.255.0.

Также возможно управление устройством через консольный порт. Для подключения к порту необходимо использовать следующие параметры терминала: 115200 бит/с, 8 бит, без проверки четности, 1 стоп-бит.

Для входа в устройство необходимо ввести имя пользователя nsg и пустой пароль. Работа с Web-интерфейсом и текстовым интерактивным интерфейсом описана в документе NSG:

Программное обеспечение NSG Linux 2.0. Руководство пользователя.

Команды интерфейса снабжены краткой встроенной справкой и развёрнутым описанием на русском и английском языках. Общее описание настроек для различных задач см. в вышеупомянутом документе.

После настройки устройство доступно для удалённого управления по сети IP.

ПРИМЕЧАНИЕ Одновременно к устройству могут иметь доступ несколько пользователей через Web-интерфейс и/или Telnet. При этом только один из них может работать в режиме конфигурирования устройства; остальным разрешается только просматривать параметры конфигурации и статистику работы устройства.

3.3. Безопасность устройства

Для предотвращения несанкционированного доступа к конфигурации устройства используется парольная защита. По умолчанию для пользователя nsg установлен пустой пароль. Перед началом эксплуатации настоятельно рекомендуется назначить устройству уникальный секретный пароль.

Для удаленного управления устройством по сетям общего пользования рекомендуется использовать HTTPS и SSH вместо HTTP и Telnet, соответственно.

ВНИМАНИЕ! ДЛЯ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К УСТРОЙСТВУ НЕОБХОДИМО УСТАНОВИТЬ УНИКАЛЬНЫЙ СЕКРЕТНЫЙ ПАРОЛЬ.
ПОМНИТЕ: ТЕ, КТО ХОЧЕТ ПРОНИКНУТЬ НА ВАШЕ УСТРОЙСТВО, ОБЫЧНО ЧИТАЮТ ДОКУМЕНТАЦИЮ ГОРАЗДО ВНИМАТЕЛЬНЕЕ ВАС!

3.4. Использование внешних устройств USB

Использование внешних устройств USB сторонних производителей, а также устройств 1–Wire, возможно только при условии, что они поддерживаются программным обеспечением NSG Linux 2.0.

При питании внешнего USB-устройства непосредственно от NSG–1000/GW ток, потребляемый этим устройством, не должен превышать 500 мА. Несоблюдение этого условия может привести к выходу из строя NSG–1000/GW. При подключении внешнего устройства с потребляемым током более 500 мА необходимо обеспечить его питание от внешнего источника.

3.5. Восстановление заводской конфигурации, модернизация ПО

Программное обеспечение устройства хранится в перезаписываемой энергонезависимой памяти (*Flash memory*) и может быть заменено другой версией по усмотрению пользователя. Замена программного обеспечения может быть необходима после выхода новой версии, при обнаружении критических ошибок в текущей версии (откат на предыдущую версию), и т.п.

Установка NSG Linux 2.0 производится по TFTP, FTP или HTTP и может быть выполнена двумя способами:

— В сервисном режиме работы системы. Существующая конфигурация устройства безусловно удаляется и заменяется заводской конфигурацией. Эта же процедура (переустановка текущей версии) используется для восстановления заводской конфигурации.

— В основном режиме работы системы, в т.ч. удалённо по сети. Существующая конфигурация устройства сохраняется, в т.ч. при замене 32-битной сборки на 64-битную или наоборот.

Если доступ к устройству невозможен по причине утраты сетевых адресов или паролей, то для восстановления заводской конфигурации также необходимо выполнить переустановку программного обеспечения в сервисном режиме.

Файлы с программным обеспечением NSG Linux могут быть загружены с Web-сайта компании по адресам:

http://www.nsg.ru/nsg-linux/binary/
ftp://ftp.nsg.net.ru/pub/nsg-linux/binary/

Программное обеспечение NSG Linux 2.0 для устройства NSG–1000/GW поставляется в виде единого файла nsg1000-i386-rootfs.tar.gz либо nsg1000-x64-rootfs.tar.gz .

ВНИМАНИЕ Перед установкой новой версии NSG Linux в основном режиме работы системы необходимо ознакомиться с документацией (файл readme_1st.txt, Приложение 1–В к Части 1 Руководства пользователя) на предмет возможной несовместимости отдельных команд старой и новой версий. В противном случае старая конфигурация может оказаться неработоспособной и после перезагрузки доступ к устройству будет утерян.

Для входа в сервисный режим необходимо:

1. Выключить электропитание устройства.
2. Подключить клавиатуру к разъёму Kbd или к любому из портов USB.
3. Подключить порт Eth0 устройства к локальной сети. Настроить на сетевом адаптере ПК любой другой адрес вида 192.168.1.*x* (*x* = 2 … 254) с маской 255.255.255.0 и подключить ПК к этой же сети.
4. Включить электропитание устройства.
5. После того, как на порту Eth0 загорится светодиод Lnk (левый), нажимать на подключенной к устройству клавиатуре клавишу "0" с интервалом 1 раз в 2 секунды в течение 30 сек. (В дальнейшем на этой клавиатуре нажимать клавиши не потребуется, она необходима только для запуска устройства в сервисном режиме.) Через 15–20 сек после этого установить HTTP-соединение с устройством по адресу 192.168.1.1.
6. Если вход на устройство по HTTP невозможен, это значит, что устройство загрузилось в обычном режиме вместо сервисного. Следует выключить устройство и повторить процедуру. Для контроля можно подключить к разъёму VGA монитор и дождаться меню из 3 пунктов, где 0-м будет вход в сервисный режим. Меню держится 4 сек, в течение этого времени нужно нажать клавишу "0".

В этом случае NSG Linux 2.0 загружается в специальном сервисном режиме, предназначенном исключительно для обновления программного обеспечения, восстановления заводской конфигурации устройства и выполнения некоторых ключевых настроек, которые являются внешними по отношению к основному программному обеспечению. Порту eth0 назначается адрес 192.168.1.1/24. Из этого режима можно выполнить повторную установку программного обеспечения, с потерей всех настроек, либо загрузить устройство без отработки сохранённой конфигурации, с минимальными заводскими настройками, и сохранить эти настройки.

ПРИМЕЧАНИЕ Другие клавиши выбора для данной серии устройств:
1 Загрузка без отработки конфигурации (Safe Mode)
2 Загрузка в штатном режиме без поддержки консольного порта
3 Загрузка в штатном режиме с поддержкой консольного порта
По умолчанию, после задержки в 4 сек. выбирается пункт 2 или 3, в зависимости от опции, установленной на странице расширенной конфигурации сервисного ПО.

Остальные процедуры установки являются общими для всех продуктов, работающих под управлением NSG Linux 2.0, и описаны в документе:

Программное обеспечение NSG Linux 2.0. Руководство пользователя. Часть 1.

Замена программного обеспечения в устройствах NSG является штатной операцией, не может привести сама по себе к необратимому повреждению устройства, и не влияет на гарантийные обязательства производителя.

ВНИМАНИЕ Запрещается отключать питание устройства или нажимать кнопку Reset во время стирания или записи энергонезависимой памяти.

3.6. Обновление ПО сервисного режима

В отдельных случаях возможны существенные доработки и изменения основного ПО NSG Linux 2.0, требующие внесения изменений не только в него самого, но и в загрузчик и в ПО сервисного режима. Обновление производится с помощью штатной процедуры установки частичных обновлений (*service packs*), предусмотренной в NSG Linux 2.0. Процедура доступна как через Web-, так и через консольный интерфейс в узле .system.software.service-pack .

ВНИМАНИЕ Замена ПО сервисного режима является критически ответственной процедурой и должна производиться только при электропитании устройства от источника бесперебойного питания. В случае отказа электропитания в ходе процедуры устройство остаётся в неработоспособном состоянии. В этом случае восстановление программного обеспечения возможно только в компании NSG, гарантия аннулируется, транспортировка устройства в NSG и обратно производится за счёт заказчика.

Выполнение процедуры описано в документе:

Программное обеспечение NSG Linux 2.0. Руководство пользователя. Часть 1.

4. Примеры конфигурации

4.1. Сервер системы *ui*TCP

Устройство NSG–1000/GW используется в качестве центрального сервера системы ***ui*TCP**, обслуживающей большое число банкоматов. Порт eth0 включён во внутреннюю сеть процессингового центра, eth1 — в сеть общего пользования. ***ui*TCP** работает в режиме TCP-прокси.

Общая конфигурация:

```
ip
: route
: : 1
: : : gateway                = "123.45.67.90"
: : : network                = "0.0.0.0/0"
port
: eth0
: : ifAddress
: : : prefix                 = "10.0.0.7/8"
: eth1
: : ifAddress
: : : prefix                 = "123.45.67.89/30"
system
: hostname                   = "uitcp_srv"
: ntp
: : enable                   = true
: : host                     = "194.149.67.129"
```

Конфигурация ***ui*TCP**: общие настройки сервера. Курсивом выделены существенные настройки, установленные по умолчанию.

```
tunnel
: uitcp
: : configure
: : : mode                   = "server"
: : : tunnelListener
: : : : host = "*"
: : : : port = 50005
```

ПРИМЕЧАНИЕ Номер порта TCP для tunnelListener должен соответствовать указанному в настройках удалённого устройства NSG (клиента ***ui*TCP**). Если сервер не подключён к сети общего пользования напрямую, а находится за входным маршрутизатором, то на этом маршрутизаторе должен быть настроен Destination NAT для данного порта.

Предполагается, что SSL задействовано и использует настройки по умолчанию, поэтому специальная конфигурация не требуется. Это подразумевает, что сертификаты X.509 сгенерированы локально с помощью скриптов cert-root, cert-server, cert-client, rehash (либо, в случае их получения в стороннем удостоверяющем центре, разложены в соответствующие директории /etc/uitcp/certs/*/).

```
: : : ssl
: : : : disable                = false
: : : : options
: : : : : all                  = true
: : : : : no_sslv2             = true
: : : : verify
: : : : : fail_if_no_peer_cert = true
: : : : : peer                 = true
```

Настройка входящих соединений от одного из банкоматов. Предполагается, что в конфигурации всех банкоматов указан типовой TCP-порт назначения на процессинговом сервере — 20000; в то же время на процессинге данный банкомат зарегистрирован под IP-адресом 10.0.1.1 и должен обращаться на порт TCP 20001 (для других банкоматов — 20002 и т.д.).

```
: : : clients
: : : : ATM001
: : : : : description          = "test ATM"
: : : : : nat
: : : : : : : 1
: : : : : : : : inDstPort      = 20000
: : : : : : : : outDstAddr     = "10.0.0.1"
: : : : : : : : outDstPort     = 20001
: : : : : : : : outSrcAddr     = "10.0.1.1"
```

Конфигурация обратных соединений из процессингового центра на удалённую площадку. Администратор, чтобы попасть на банкомат, обращается к серверу NSG по адресу 10.0.0.7 и номеру порта TCP 30001 (для других площадок — 30002 и т.д.) в локальной сети банка; это соединение принимается сервером *ui*TCP и транслируется на удалённую площадку. Для соединения с удалённым устройством NSG (клиентом ***ui*TCP**) администратор обращается по адресу 10.0.0.7 и номеру порта TCP 40001 (40002 и т.д.)

```
: : : : : localListener
: : : : : : : 1
: : : : : : : : host      = "10.0.0.7"
: : : : : : : : port      = 30001
: : : : : : : 2
: : : : : : : : host      = "10.0.0.7"
: : : : : : : : port      = 40001
```

ВНИМАНИЕ Настройка узлов local-listener производится на стороне, инициирующей TCP-соединения, парных к ним узлов nat — на стороне, принимающей эти соединения.

4.2. Сервер доступа IPsec с NAT–T и X.509

Устройство NSG–1000/GW используется в центральном офисе в качестве шлюза VPN, к которому подключаются удалённые филиалы по IPsec. При этом само оно находится внутри сети офиса, за входным маршрутизатором, на котором настроен Destination NAT для портов UDP 500 и 4500. Филиалы могут иметь динамические адреса, а также приватные адреса в сети поставщиков услуг, и выходить в Интернет через NAT. Таким образом, IP-адреса клиентов, под которыми они видны в Интернет, априори неизвестны, неинформативны и также могут не соответствовать их фактическим адресам, под которыми они известны сами себе.

Традиционный механизм аутентификации сторон и защиты данных с помощью PSK на сегодняшний день является достаточно надёжным только при условии статических IP-адресов обеих сторон (т.е. когда каждая сторона фактически аутентифицируется по совокупности реквизитов IP-адрес + PSK); применять его для произвольных адресов (0.0.0.0) не рекомендуется. По этой причине используется механизм аутентификации на основе асимметричной пары RSA-секретов, подтверждённых сертификатами X.509.

Конфигурация устройства. В данном случае "левой" стороной туннеля считается к**Л**иент, "правой" стороной — се**Р**ве**Р** (для удобства запоминания). Для большей ясности, вопреки традиционной для Linux избыточной и симметричной конфигурации, приведены только параметры, используемые по существу. NAT Traversal, по умолчанию, включёно.

Приватный ключ самого устройства NSG находится в файле /etc/ipsec.d/private/nsg1000gw_pvtkey.pem, а пароль от него записан в параметр secret. Сертификат хранится в файле /etc/ipsec.d/certs/nsg1000gw_cert.pem, при этом строка rightid должна строго соответствовать всем перечисленным полям сертификата сервера, а leftid — сертификата соответствующего клиента. Помимо этих двух файлов, для работы системы X.509 нужен, как минимум, ещё один файл — корневой сертификат, который хранится в файле /etc/ipsec.d/cacert/root.pem .

```
        ip
        : route
        : : 1
        : : : gateway                   = "192.168.1.1"
        : : : network                   = "0.0.0.0/0"
        port
        : eth0
        : : ifAddress
        : : : prefix                    = "10.0.0.7/24"
        : eth1
        : : ifAddress
        : : : prefix                    = "192.168.1.2/24"
        system
        : ntp
        : : enable                      = true
        : : host                        = "194.149.67.129"
        tunnel
        : ipsec
        : : enable                      = true
        : : secrets
        : : : rsa
        : : : : 1
        : : : : : file                  = "nsg1000gw_pvtkey.pem"
        : : : : : secret                = "qwerty"
        : : connections
        : : : %default
        : : : : authby                  = "rsasig"
        : : : : esp
        : : : : : 3des-md5              = "true"
        : : : : left                    = "%any"
        : : : : leftrsasigkey           = "%cert"
        : : : : right                   = "192.168.1.2"
        : : : : rightid                 = "/C=RU/ST=MO/L=Moscow/O=MMM/OU=      ↵
users_dept/CN=MMM_server/emailAddress=users@mmm.ru"
        : : : : rightcert               = "nsg1000gw_cert.pem"
        : : : : rightnexthop            = "123.45.67.90"
        : : : : rightsourceip           = "10.0.0.7"
        : : : : rightsubnet             = "10.0.0.0/24"
        : : : branch1
        : : : : auto                    = "add"
        : : : : leftid                  = "/C=RU/ST=MO/L=Moscow/O=MMM/OU=      ↵
users_dept/CN=MMM_branch1/emailAddress=users@mmm.ru"
        : : : : leftsubnet              = "10.1.1.0/24"
        : : : branch2
        ……
```

Конфигурация устройства (например, NSG–605, NSG–700) в качестве клиента. Детали работы публичного интерфейса s1 и того, каким образом создаётся маршрут по умолчанию через него, в данном случае не существенны и потому опущены.

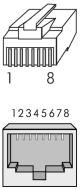
```
ip
: route
: : 1
: : : device                    = "s1"
: : : network                   = "0.0.0.0/0"
port
: eth0
: : ifAddress
: : : prefix                    = "10.1.1.1/24"
: s1
.....................................
system
: ntp
: : enable                      = true
: : host                        = "194.149.67.129"
tunnel
: ipsec
: : enable                      = true
: : secrets
: : : rsa
: : : : 1
: : : : : file                  = "branch1_pvtkey.pem"
: : : : : secret                = "123456"
: : connections
: : : branch1
: : : : authby                  = "rsasig"
: : : : auto                    = "start"
: : : : esp
: : : : : 3des-md5              = "true"
: : : : left                    = "%defaultroute"
: : : : leftnexthop             = "%defaultroute"
: : : : leftcert                = "branch1_cert.pem"
: : : : leftsourceip            = "10.1.1.1"
: : : : leftsubnet              = "10.1.1.0/24"
: : : : right                   = "123.45.67.89"
: : : : rightid                 = "/C=RU/ST=MO/L=Moscow/O=MMM/OU=
users_dept/CN=MMM_server/emailAddress=users@mmm.ru"
: : : : rightrsasigkey          = "%cert"
: : : : rightsubnet             = "10.0.0.0/24"
```

ПРИМЕЧАНИЕ В данной реализации IPsec идентификатор клиента (leftid) на самом клиенте не требуется по существу, однако на стороне сервера они обязательны оба. Во избежание ошибок рекомендуется всегда указывать оба идентификатора на обеих сторонах.

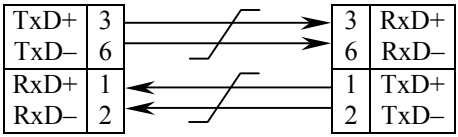
5. Назначение контактов и распайка кабелей для фиксированных портов

Порты Ethernet (RJ–45)	
№	**Сигнал**
1	TxD+
2	TxD–
3	RxD+
4	Не используется
5	Не используется
6	RxD–
7	Не используется
8	Не используется

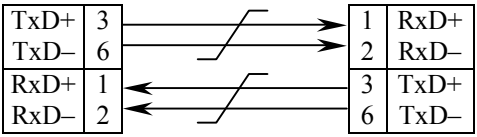
Консольный порт (DB–9m)	
№	**Сигнал**
1	Ready In
2	Data In
3	Data Out
4	Ready Out
5	GND
6	Не используется
7	Flow Control Out
8	Flow Control In
9	Не используется



Кабель "Ethernet RJ–45 straight" (серый или синий)

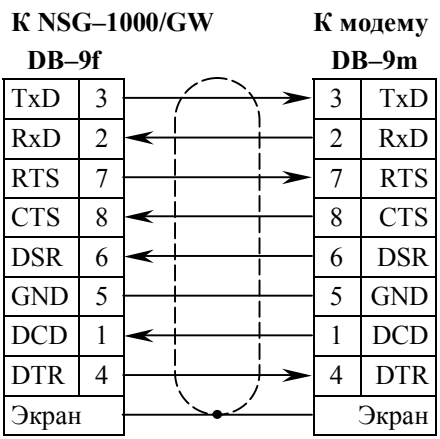


Кабель "Ethernet RJ–45 crossover" (зеленый)

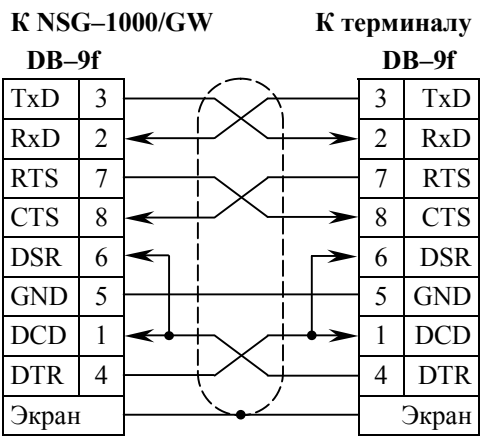


Подключение к коммутатору локальной сети производится прямым кабелем; к ПК — перекрёстным кабелем.

модемный кабель



нуль-модемный кабель CAV–V24/D9/FC/A



6. Комплект поставки

Устройство NSG–1000/GW	1 шт.
Кабель "Ethernet RJ–45 straight" (синий, серый)	1 шт.
Кабель "Ethernet RJ–45 crossover" (зеленый)	1 шт.
Консольный (нуль-модемный) кабель CAV–V24/D9/FC/A	1 шт.
Кабель питания 110–220 В	1 шт.
Паспорт устройства	1 шт.
CD-ROM с документацией	1 шт.

ООО «Эн–Эс–Джи»
Россия 105187 Москва
ул. Вольная, д.35
Тел./факс: (+7–495) 727–19–59 (многоканальный)

http://www.nsg.ru/
mailto:info@nsg.net.ru
mailto:sales@nsg.net.ru
mailto:support@nsg.net.ru