



Устройство однонаправленной передачи данных
аппаратно-программный комплекс InfoDiode SMART light
(наименование и индекс изделия)

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

RU.29318444.00003-01 92

AMTID-SMRT-BKL-100

(обозначение)

2026 г.

Содержание

1. Введение	3
2. Технические характеристики АПК InfoDiode SMART light.....	4
2.1 Габариты.....	4
2.2 Электропитание, мощность и тепловыделение	4
2.3 Условия эксплуатации	4
2.4 Интерфейсы	4
3. Комплектация	6
3.1 Подключение АПК InfoDiode SMART	11
3.1.1 Подключение к электрической сети, включение эл. питания.....	11
3.1.2 Межблочная коммутация.....	11
3.1.3 Подключение Изделия к сети	12
3.1.4 Организация доступа для выполнения настройки IN и OUT частей.....	12
4. Сведения об актуальных версиях АПК InfoDiode SMART light	16
5. Настройка InfoDiode SMART light для передачи прикладного трафика.....	17

1. Введение

Настоящее руководство содержит инструкцию по подготовке к эксплуатации оборудования АПК InfoDiode SMART light и его первоначальной настройке.

Монтаж оборудования должен производиться с учетом соблюдения всех технических требований и характеристик АПК InfoDiode SMART light.

2. Технические характеристики АПК InfoDiode SMART light

2.1 Габариты

АПК InfoDiode SMART light представляет собой единую аппаратно-программную платформу однонаправленной передачи данных, состоящую из трех блоков (IN, DIODE, OUT).

В Таблица 1 приведены габаритные характеристики АПК InfoDiode SMART light.

Таблица 1. Габаритные характеристики АПК InfoDiode SMART light

	Ширина (мм)	Глубина (мм)	Высота (мм)	Вес (кг)
АПК InfoDiode SMART light	135	158	120	2

2.2 Электропитание, мощность и тепловыделение

Требования АПК InfoDiode SMART light по электропитанию:

- 10 – 30 В (DC)
- Max 32 Вт

На каждом блоке IN и OUT АПК InfoDiode SMART light реализованы по 2 отдельных разъема для подключения электропитания. Допускается подключение разных разъемов блока к отдельным источникам электропитания с целью обеспечения резервирования по электропитанию, при этом электропитание блока будет осуществляться от разъема с более высоким входным напряжением. Между разными разъемами блоков отсутствует гальваническая развязка, вывод «-» является общим.

Блок DIODE имеет 2 независимых разъема электропитания PS1 и PS2 на передней панели. Оба разъема имеют защиту от неправильной полярности подключения электропитания и гальванически развязаны между собой. Электропитание блока DIODE может осуществляться:

- одновременно с двух разъемов PS1 и PS2 на передней панели – режим резервированного электропитания;
- с любого из разъемов PS1, PS2 на передней панели.

2.3 Условия эксплуатации

- Рабочая температура от +0°C до +40°C
- Температура хранения от -40°C до +70°C
- Влажность 5% - 95% (без конденсата)

2.4 Интерфейсы

Каждый блок (IN и OUT) АПК InfoDiode SMART light содержит:

- 2 x USB 3.0 (Type-A);
- 1 x HDMI;

- 1 x USB Type-C (Serial console);
- 2 x Ethernet 10/100/1000 Base-T (RJ-45).

Блок DIODE АПК InfoDiode SMART light:

- 2 x Ethernet 10/100/1000 Base-T (RJ-45).

3. Комплектация

В комплектацию АПК InfoDiode SMART light входят:

- Два блока промышленных компьютеров (IN и OUT);
- Блок DIODE (устройство однонаправленной передачи данных).

На Рисунок 1 изображена передняя панель устройства однонаправленной передачи данных АПК InfoDiode SMART light в составе трех блоков:

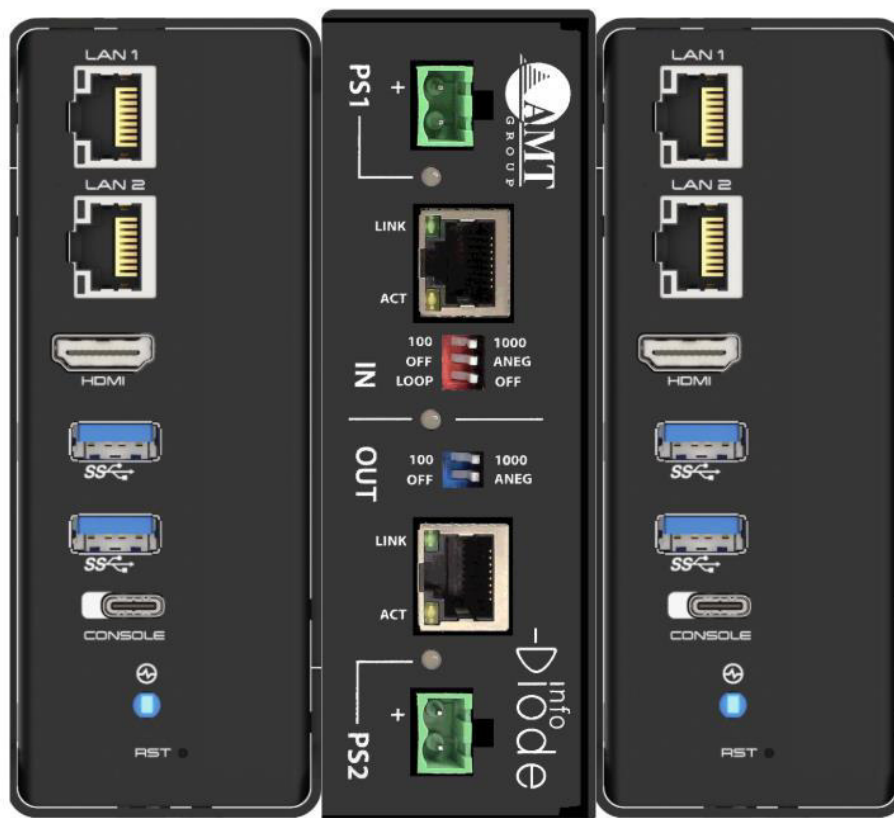


Рисунок 1. Передняя панель устройства однонаправленной передачи данных АПК InfoDiode SMART light в составе трех блоков

На Рисунок 2 изображена задняя панель устройства однонаправленной передачи данных АПК InfoDiode SMART light в составе трех блоков. Панель предназначена для крепления АПК InfoDiode SMART light на монтажную DIN-рейку 35 мм.

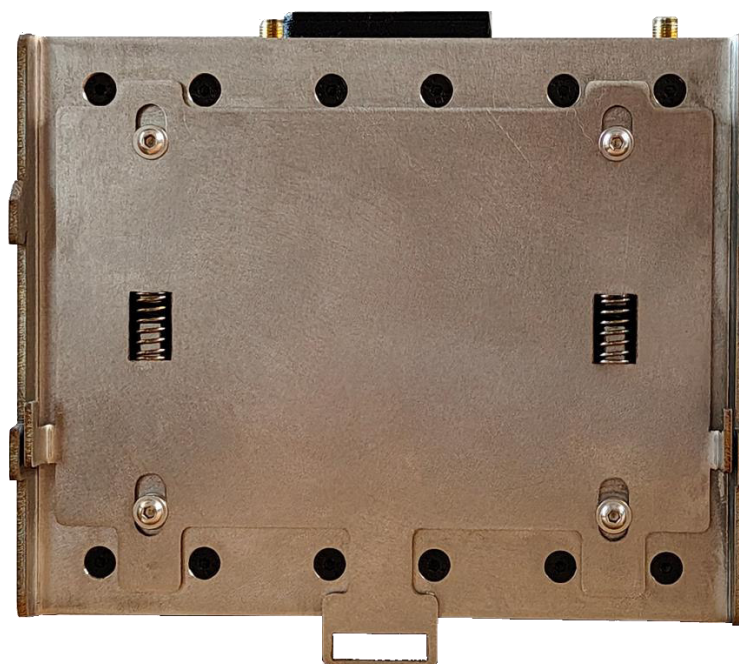


Рисунок 2. Задняя панель АПК InfoDiode SMART light в составе трех блоков

Ниже показаны схематичные изображения Изделия: вид спереди (Рисунок 3), вид сверху (Рисунок 4) и вид снизу (Рисунок 5).

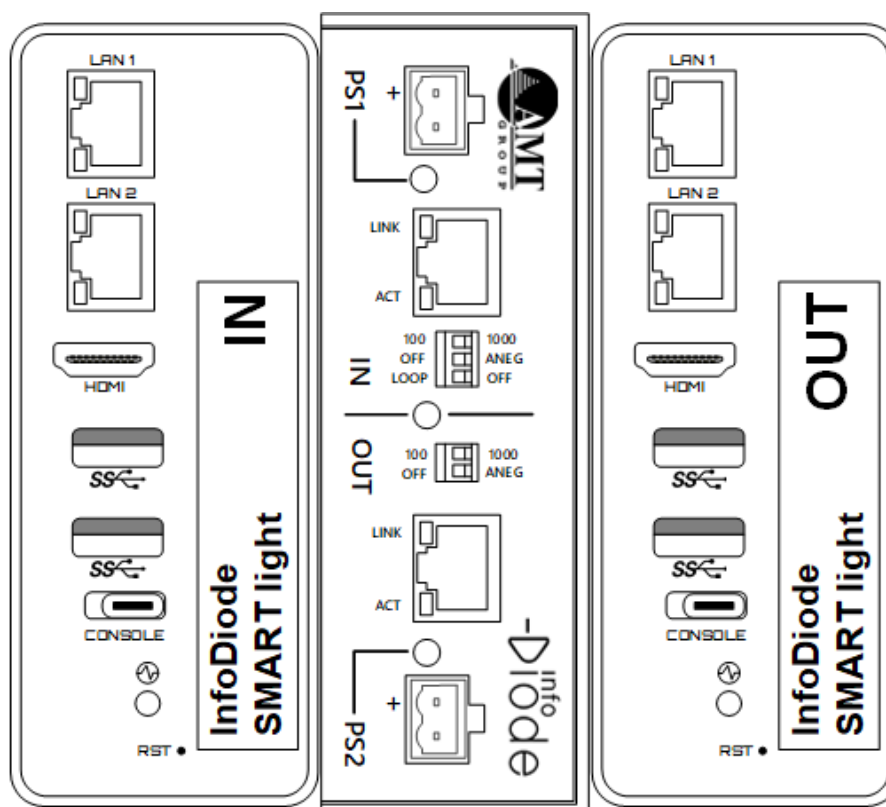


Рисунок 3. Схема вида спереди

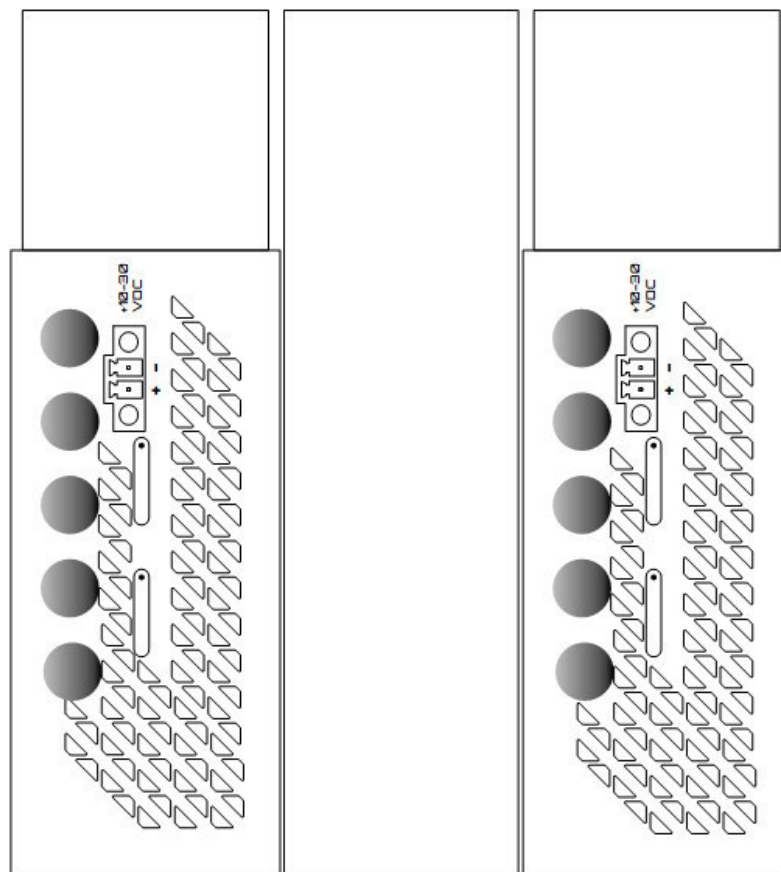


Рисунок 4. Схема вида сверху

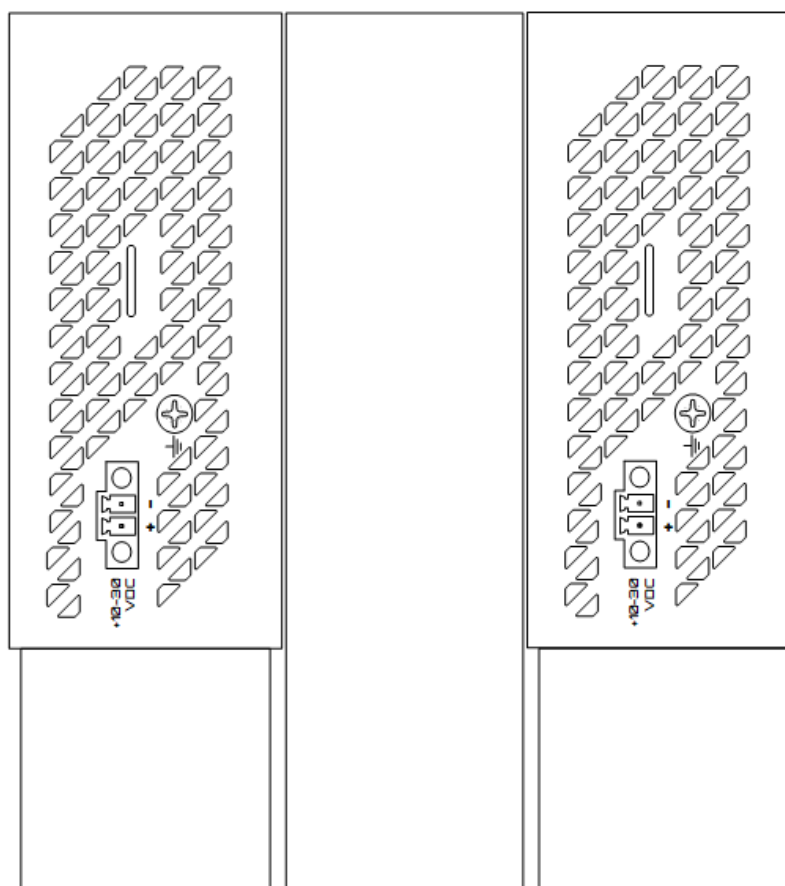


Рисунок 5. Схема вида снизу

Изделие выполнено в виде аппаратно-программного комплекса, состоящего из трех блоков, слева направо: IN-часть, DIODE, OUT-часть. Блоки объединены в единую конструкцию с помощью задней панели¹.

На передней панели блоков IN- и OUT-частей расположены LED индикаторы статуса электропитания, совмещенные с кнопкой включения, а также отверстие кнопки “Reset”, коннектор Type-C для подключения Serial консоли, 2 порта USB 3.0 (Type-A), коннектор HDMI для подключения дисплея, 2 порта Ethernet 100Base-TX/1000Base-T (RJ-45). Сверху и снизу блоков IN и OUT расположены коннекторы для подключения электропитания постоянного тока 10-30 VDC, потребляемая каждым блоком мощность не более 10W без учета внешних потребителей USB.

На передней панели блока DIODE расположены LED индикаторы:

- статуса электропитания PS1
 - Индикатор горит зеленым цветом при наличии напряжения электропитания на разъеме PS1 и исправности встроенного конвертера электропитания.
 - Индикатор не горит при отсутствии напряжения электропитания на разъеме PS1 или неисправности встроенного конвертера электропитания, но при наличии электропитания на разъеме PS2.
- статуса электропитания PS2
 - Индикатор горит зеленым цветом при наличии напряжения электропитания на разъеме PS2 и исправности встроенного конвертера электропитания.
 - Индикатор не горит при отсутствии напряжения электропитания на разъеме PS2.
- статуса внешнего интерфейса соответствующего контура (LINK)
 - Индикатор не горит при отсутствии связи с подключенным оборудованием.
 - Индикатор горит при наличии связи с подключенным оборудованием.
- активности внешнего интерфейса соответствующего контура (ACT)
 - Для входного (IN) контура – индикатор горит при получении данных от подключенного оборудования.
 - Для выходного (OUT) контура – индикатор горит при отправке данных на подключенное оборудование.
 - Индикатор не горит при отсутствии передаваемых данных.
- статуса внутреннего канала между входным и выходным контурами.
 - Индикатор не горит при отсутствии связи на стыке входного и выходного контуров.

¹ Конструкция объединения блоков IN, DIODE, OUT определяется Изготовителем

- Индикатор горит зеленым цветом при наличии связи на стыке входного и выходного контуров.
- Индикатор горит красным цветом при отсутствии или неисправности внутренних оптических модулей

Кроме индикаторов на передней панели блока DIODE расположены два внешних интерфейса 100Base-TX/1000Base-T – с RJ45-модулями: входной (IN) и выходной (OUT), два разъема PS1 и PS2 для подключения источников электропитания постоянного тока 10-36 VDC, max 12 W и конфигурационные переключатели для каждого из IN и OUT модулей.

При настройке Изделия задокументируйте в Таблица 2 все настройки оборудования АПК InfoDiode SMART light. Эти данные могут понадобиться для администрирования и резервного восстановления.

Таблица 2. Настройки оборудования АПК InfoDiode SMART light

Пункт	Описание	Ваша настройка	
		IN	OUT
IP-адрес и маска сетевых интерфейсов	IP-адрес и маска интерфейсов для доступа по SSH и для целей передачи данных.	Управление и Данные	
Маршрут по умолчанию (шлюз)	Сетевой шлюз, на который пакет отправляется в том случае, если маршрут к сети назначения пакета не известен		
Domain name server *необязательно	IP-адрес сервера, используемый для DNS запроса		
Административные данные *необязательно	Логин и пароль для доступа по SSH. После авторизации можно изменить		

3.1 Подключение АПК InfoDiode SMART

3.1.1 Подключение к электрической сети, включение эл. питания

Подключите Изделие к эл. питанию и включите кнопки эл. питания на блоках IN и OUT. Устройство готово для подключения к сети.

3.1.2 Межблочная коммутация

Для правильного функционирования Изделия необходимо выполнить межблочную коммутацию. Для этого:

1. Подключите интерфейс LAN2 блока IN к интерфейсу IN блока DIODE кабелем вида «витая пара» с коннекторами RJ-45.
2. Подключите интерфейс OUT блока DIODE к интерфейсу LAN2 блока OUT кабелем вида «витая пара» с коннекторами RJ-45.

Схема межблочной коммутации Изделия показана на Рисунок 3.

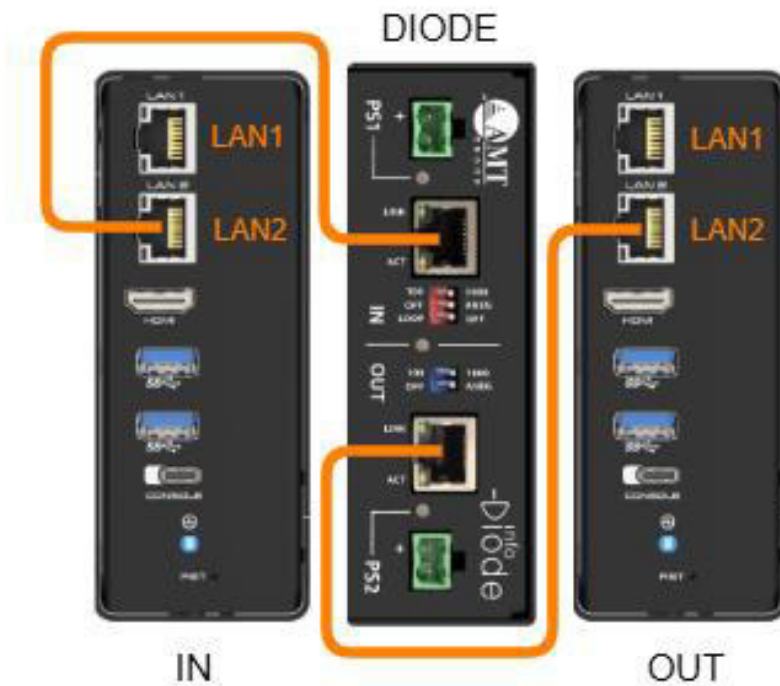


Рисунок 6. Схема межблочной коммутации Изделия

3.1.3 Подключение Изделия к сети

1. Подключите интерфейс внешнего сетевого оборудования к интерфейсу LAN1 блока IN кабелем вида «витая пара» с коннекторами RJ-45.
2. Подключите интерфейс данных LAN1 блока OUT к внешнему сетевому оборудованию (или к конечному устройству) кабелем вида «витая пара» с коннекторами RJ-45.

На Рисунок 7 представлена схема подключения АПК InfoDiode SMART light к корпоративной сети:

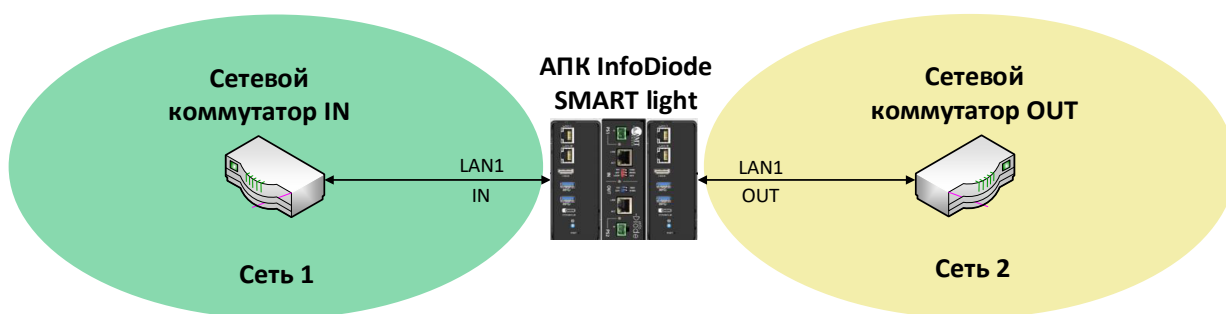


Рисунок 7. Схема подключения АПК InfoDiode SMART light к корпоративной сети

3.1.4 Организация доступа для выполнения настройки IN и OUT частей

Просмотр и изменение конфигурации IN- и OUT-частей АПК InfoDiode SMART light возможно при подключении к устройству одним из трех способов:

1. Локально – на месте. Подключиться по serial console физически к соответствующей части АПК InfoDiode SMART light, используя порт Type-C USB. Параметры подключения представлены на примере утилиты MobaXterm²:
 - a. Serial engine: PuTTY (allow manual port setting)
 - b. Speed: 115200
 - c. Data bits: 8
 - d. Stop bits: 1
 - e. Parity: None
 - f. Flow control: None
2. Локально – на месте. Подключить монитор и клавиатуру физически к соответствующей части (IN- и OUT-части) АПК InfoDiode SMART light, используя порты USB и HDMI. Этот способ подключения должен использоваться в случае касающихся аварийного восстановления BIOS. Для функций управления (если требуется локальное подключение) следует использоваться способ 1 – подключение через serial console.
3. Удаленно. Получить доступ по протоколу SSH, обеспечив подключение по порту Ethernet 10/100/1000Base-T. В частности, для доступа к той или иной части АПК InfoDiode SMART light (IN- и OUT-части) по протоколу SSH необходимо, чтобы предварительно был настроен корректный IP-адрес на сетевом ethernet-интерфейсе АПК InfoDiode SMART light, был установлен маршрут по умолчанию – см. раздел «Организация доступа по протоколу SSH».

Для начала настройки устройства:

1. Подключитесь последовательно к IN- и OUT-части АПК InfoDiode SMART light напрямую с внешнего ПК по SSH. После подключения введите в терминале логин и пароль пользователя “diode”.
2. После авторизации на IN- и OUT-частях АПК InfoDiode SMART light под аккаунтом “diode” **рекомендуется создать на каждой части нового пользователя ОС и включить его в группу “sudo”**.

Внимание!

После установки InfoDiode Smart light необходимо:

Войти в систему под пользователем “diode” с помощью пароль по умолчанию “P@ssw0rd”. При первой аутентификации рекомендуется сменить пароль пользователя на новый, соответствующий политикам безопасности Вашей организации. По умолчанию пароль должен соответствовать следующим критериям: не менее 8 символов, должен содержать: заглавные буквы, строчные буквы, цифры и специальные символы, без повторяющихся символов. Запомните или зафиксируйте данный пароль согласно правилам и политикам безопасности для вашей организации, т.к. он может быть использован в качестве резервного для восстановления доступа к АПК.

² В ОС семейства Linux рекомендуется использовать программное обеспечение Minicom.

При необходимости создайте системных пользователей, которые будут использоваться в дальнейшем для администрирования системы.

Создать пользователя можно с помощью команды `useradd -G sudo -m -s /bin/bash <имя пользователя>`, например: `useradd -G sudo -m -s /bin/bash aivanov`

Задать пароль с помощью команды `passwd <имя пользователя>`, например: `passwd aivanov`

В InfoDiode Smart light наличие пользователя в группе “sudo” означает возможность повышения привилегий с помощью одноименной системной команды “sudo”.

В целях безопасности пользователю “root” не задан пароль и запрещен удаленный доступ по SSH. Не рекомендуется осуществлять работу непосредственно под пользователем “root”.

Организация доступа по протоколу SSH

При подключении (последовательно) к сторонам IN- и OUT АПК InfoDiode SMART light:

1. Требуется создать резервную копию конфигурации сетевой подсистемы `/etc/systemd/network/10-data.network`. Открыть файл конфигурации сетевой подсистемы редактором `vim` с повышением привилегий `sudo` и вместо преднастроенных значений указать в секциях [Network] и [Route] корректные IP-адрес и маску сети, шлюз по-умолчанию, адрес DNS и имя домена, адрес сервера NTP.

```
[Match]
Name=data

[Network]
Address=10.0.141.192/24
Gateway=10.0.141.1
DNS=10.0.101.14
Domains=dev.amt.ru
NTP=0.ru.pool.ntp.org
```

Рисунок 8. Конфигурация сетевой подсистемы

2. Выполнить перезапуск службы сети командой:
`sudo systemctl restart systemd-resolved.service systemd-networkd.service.`
3. Дальнейшие работы для каждой стороны IN- и OUT АПК InfoDiode SMART light можно проводить удаленно, выполняя подключение по протоколу SSH.

Внимание!

Под пользователем “root” нельзя зайти по протоколу SSH на IN- и OUT-части АПК InfoDiode SMART light до тех пор, пока ему не будет задан пароль и в настройках это не будет явно разрешено.

Выполнение других настроек и конфигурирование правил передачи данных через АПК InfoDiode SMART light выполняется в файлах конфигурации для каждой из частей IN- и OUT АПК InfoDiode SMART light соответственно – см. раздел 5 настоящего документа.

4. Сведения об актуальных версиях АПК InfoDiode SMART light

Производитель публикует сведения, касающиеся выпуска актуальных версий АПК InfoDiode SMART light, оказания технической поддержки и действующих сертификатов ФСТЭК России, на официальном сайте <https://infodiode.ru/>. Публикации подлежат следующие сведения:

- Об актуальной версии ПО блоков IN и OUT АПК InfoDiode SMART light;
- Об версиях ПО блоков IN и OUT АПК InfoDiode SMART light, на которые осуществляется полная техническая поддержка и сопровождение;
- О версиях ПО блоков IN и OUT АПК InfoDiode SMART light, техническая поддержка на которые в перспективе будет завершена и для которых осуществляется только поддержка безопасности средства, включающая устранение недостатков, дефектов, критических уязвимостей и недеklarированных возможностей;
- О версиях АПК InfoDiode SMART light, сертификат ФСТЭК России которых в перспективе будет отозван или закончит свое действие.

Администратор АПК InfoDiode SMART light должен не реже чем раз в 6 месяцев осуществлять контроль актуальности версии продукта в целях предупреждения нарушений законодательства Российской Федерации в части использования СЗИ, в отношении которых не осуществляется техническая поддержка или поддержка безопасности средства, либо окончено действие сертификата ФСТЭК России.

5. Настройка InfoDiode SMART light для передачи прикладного трафика

Выполнение других настроек и конфигурирование правил передачи данных через АПК InfoDiode SMART light выполняется согласно Приложению 1 настоящего документа.

Инструкция по настройке конкретных сервисов передачи (файлов, Modbus трафика, UDP, RAW TCP) через InfoDiode SMART light представлена в соответствующих инструкциях коннекторов и инструкциях по организации передачи типов трафика.

Приложение 1. Настройка InfoDiode SMART light

Оглавление

1. Важная информация	19
2. Настройка сетевых устройств и IP адресов устройства	19
3. Настройка имени узла	20
4. Настройка системных пользователей	21
4.1 Добавление системного пользователя	21
4.2 Удаление системного пользователя	22
4.3 Смена пароля системного пользователя	22
4.4 Принудительная смена пароля при следующем входе	22
4.5 Политика безопасности в отношении паролей	22
4.5.1 Попытки аутентификации и параметры блокирования	22
4.5.2 Сложность пароля	23
4.5.3 Количество предыдущих хеш паролей для сравнения	23
4.5.4 Срок действия пароля	23
4.6 Аутентификация с помощью SSH-ключа с паролем (двухфакторная аутентификация)	23
4.6.1 Загрузка PuTTY, распаковка на флэш-диск	23
4.6.2 Генерация ключей, задание пароля для закрытого ключа	24
4.6.3 Перенос открытого ключа на сервер	24
4.6.4 Настройка PuTTY для аутентификации с помощью ключа	25
4.6.5 Подключение к серверу с использованием ключа и пароля	25
4.6.6 Изменение пароля ключа	26
4.6.7 Изменение настроек InfoDiode SMART для запрета аутентификации с использованием пароля	26
4.7 Отключение доступа по SSH	27
5. Настройка системных сервисов	27
5.1 Настройка брандмауэра	27
5.2 Конфигурирование NTP и параметров таймзоны	28
5.3 Настройка сервиса мониторинга	29
6. Настройка коннекторов	29
7. Мониторинг, диагностика, контроль состояния	29
7.1 Просмотр событий при доступе через SSH / Serial	29

7.2	Передача данных журнала на внешний сервер по протоколу syslog	31
8.	Обновление пакетов ОС и ПО коннекторов	32
8.1	Обновление пакетов ОС	32
8.2	Обновление коннекторов	32

1.Важная информация

Операции администрирования, связанные с настройкой АПК InfoDiode SMART light, необходимо выполнять с повышением привилегий с помощью команды `sudo`.

Например: `sudo reboot`.

Для использования команды `sudo` пользователь должен состоять в группе `sudo`.

Например, чтобы добавить пользователя `username` в группу `sudo` необходимо выполнить:
`sudo usermod -a -G sudo username`

Для удаления пользователя `username` из группы `sudo`:
`sudo gpasswd -d username sudo`

АПК InfoDiode SMART light поставляется с предустановленными файлами лицензий для каждого экземпляра ПО коннекторов.

Внимание! Чтобы избежать ошибок при запуске ПО, **запрещено удалять:**

- Файлы лицензий `.lic` из директорий коннектора в каталоге `/etc`
- Домашние каталоги пользователей, от имени которых запускаются коннекторы
- Активационные файлы `.act_code` в этих домашних каталогах (их повторная генерация также аналогична удалению)

В случае удаления этих элементов для восстановления работы АПК потребуется привлечение специалистов производителя.

2.Настройка сетевых устройств и IP адресов устройства

АПК InfoDiode SMART light поставляется с шаблонами настроек сетевых интерфейсов.

Каждая сторона (IN и OUT-часть) АПК InfoDiode SMART light имеет 2 физических сетевых интерфейса, в чем можно убедиться по выводу команды `ip a`.

На IN-стороне данные интерфейсы в ОС имеют названия `diode-in` и `data`, тогда как на OUT-стороне `diode-out` и `data`. Следует правильно трактовать функциональное назначение этих интерфейсов: интерфейс `data` предназначен для взаимодействия с внешними системами и отвечает за передачу данных и административное управление. Интерфейсы `diode-in` и `diode-out` на IN и OUT-сторонах соответственно являются внутренними и отвечают за однонаправленную передачу данных между IN и OUT-

частями. Все параметры внутренних интерфейсов `diode-in` и `diode-out` уже предварительно настроены на этапе стейджинга **InfoDiode SMART light**, изменение их настроек при штатной работе АПК не требуется и может привести к нарушению его функционирования. Пункты 1-3, указанные далее, отвечают за корректное именование сетевых интерфейсов в ОС и выполняются на этапе подготовки АПК перед отправкой Заказчику. Таким образом, при штатном функционировании АПК, может возникнуть необходимость только в изменении IP-адресов/маршрутизации на интерфейсе `data`, что описано в пункте 4, пункты 1-3 выполнять не требуется.

Для корректной работы этих шаблонов, требуется прописать MAC-адреса сетевых интерфейсов конкретного узла и осуществить настройку сети в соответствии с окружением:

1. С помощью команды `ip a` определить MAC-адреса сетевых интерфейсов;
2. Прописать в поле `MACAddress` адрес внешнего сетевого интерфейса, используемого для взаимодействия с внешними клиентами, в файл `/etc/systemd/network/10-data.link`;
3. Прописать в поле `MACAddress` адрес внутреннего сетевого интерфейса, используемого для взаимодействия между узлами АПК **InfoDiode SMART light**, в файл:
 1. `/etc/systemd/network/10-diode-in.link` — при настройке узла IN;
 2. `/etc/systemd/network/10-diode-out.link` — при настройке узла OUT.
4. Указать настройки сети внешнего сетевого интерфейса в файле `/etc/systemd/network/10-data.network`. Пример содержимого данного файла конфигурации приведен ниже:
5. `[Match]`
6. `Name=data`
- 7.
8. `[Network]`
9. `Address=10.0.141.126/24`
10. `Gateway=10.0.141.1`
11. `DNS=77.88.8.8`
`DNS=77.88.8.1`

Для корректного применения настроек необходимо перезагрузить узел с помощью команды `reboot`.

3. Настройка имени узла

Для задания имени узла следует использовать команду `hostnamectl`, а само имя задавать в формате **FQDN**, например:

```
hostnamectl set-hostname idsmartlight-1-in
```

После переименования узла следует скорректировать имя узла в файле `/etc/hosts`, например:

```
127.0.0.1      localhost
10.0.141.126   idsmartlight-1-in

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

Для корректного применения настроек необходимо перезагрузить узел с помощью команды `reboot`.

Эти операции уже выполнены по умолчанию производителем АПК InfoDiode SMART light по результатам операций стейджинга и требуются только в иных случаях. В обычной ситуации — выполнять не требуется.

4. Настройка системных пользователей

При поставке в АПК InfoDiode SMART light существует только один доступный для входа пользователь `diode`, входящий в группу `sudo`, доступ под этим пользователем возможен по SSH.

Войти в систему под пользователем `diode` можно с помощью пароля *по умолчанию*: `P@ssw0rd`.

После 1-й авторизации рекомендуется сменить пароль пользователя на новый, соответствующий политикам безопасности Вашей организации, но соответствующий следующим критериям: не менее 8 символов, должен содержать: заглавные буквы, строчные буквы, цифры и специальные символы, без повторяющихся символов.

4.1 Добавление системного пользователя

1. Создать пользователя с помощью команды `useradd -G sudo -m -s /bin/bash <имя пользователя>`, например:

```
useradd -G sudo -m -s /bin/bash aivanov
```

2. Задать пароль с помощью команды `passwd <имя пользователя>`, например:

```
passwd aivanov
```

В АПК InfoDiode SMART light наличие пользователя в группе `sudo` означает возможность повышения привилегий с помощью одноименной системной команды `sudo`.

4.2 Удаление системного пользователя

Для удаления пользователя необходимо выполнить команду `userdel --remove <username>`, например:

```
userdel --remove aivanov
```

4.3 Смена пароля системного пользователя

Для смены пароля пользователя необходимо выполнить команду `passwd <имя пользователя>`, например:

```
passwd aivanov
```

4.4 Принудительная смена пароля при следующем входе

Для принудительной смены пароля при следующем входе следует выполнить команду `passwd --expire <имя пользователя>`, например:

```
passwd --expire root
```

4.5 Политика безопасности в отношении паролей

Установлены следующие требования к хранению паролей и попыток аутентификации *по умолчанию*:

1. Количество неправильных вводов пароля — **4 попытки**;
2. Время измерения — **5 минут**;
3. Время блокировки — **30 минут**;
4. Количество хранимых старых паролей — **10 паролей**;
5. Длина пароля не менее восьми символов, алфавит пароля **не менее 70**;
6. Срок действия пароля — **99999 дней**.

Первые три параметра следует интерпретировать как *"Если в течении 5 минут 4 раза был введен неправильный пароль, то учетная запись пользователя, под которым осуществлялся ввод, блокируется на 30 минут."*

4.5.1 Попытки аутентификации и параметры блокирования

/etc/security/faillock.conf

```
# Количество последовательных неудачных попыток аутентификации, после  
которого доступ пользователя будет заблокирован.  
deny = 4
```

```
# Длина интервала, в течение которого должны произойти последовательные сбои
аутентификации для блокировки учетной записи пользователя (в секундах).
fail_interval = 300
```

```
# Интервал времени, после которого доступ будет снова разрешён (в секундах).
Значение 0 означает, что доступ разблокируется только вручную.
unlock_time = 1800
```

4.5.2 Сложность пароля

/etc/security/pwquality.conf

```
# Минимальное количество классов символов для нового пароля (цифры, прописные
буквы, строчные буквы, другие символы).
minclass = 4
```

4.5.3 Количество предыдущих хеш паролей для сравнения

/etc/security/pwhistory.conf

```
# Количество прошлых хешей паролей для сравнения.
remember = 10
```

4.5.4 Срок действия пароля

/etc/login.defs

```
# Срок действия пароля, после которого система попросит его изменить (в
днях).
PASS_MAX_DAYS 99999
```

4.6 Аутентификация с помощью SSH-ключа с паролем (двухфакторная аутентификация)

Аутентификация с помощью SSH-ключа подразумевает генерацию пары ключей, закрытого и открытого, при которой создается заданный пользователем пароль. Тем самым реализуется двухфакторная аутентификация, поскольку для успешной аутентификации необходимо выполнение двух условий (факторов): наличие файла ключа и ввод правильного пароля.

Для использования аутентификации с помощью SSH-ключа могут применяться различные реализации ssh-терминалов. Ниже приведена последовательность настройки двухфакторной аутентификации при использовании свободного ПО [PuTTY](#) в среде Windows, при этом программа PuTTY и файл ключа хранятся на USB флэш-диске.

4.6.1 Загрузка PuTTY, распаковка на флэш-диск

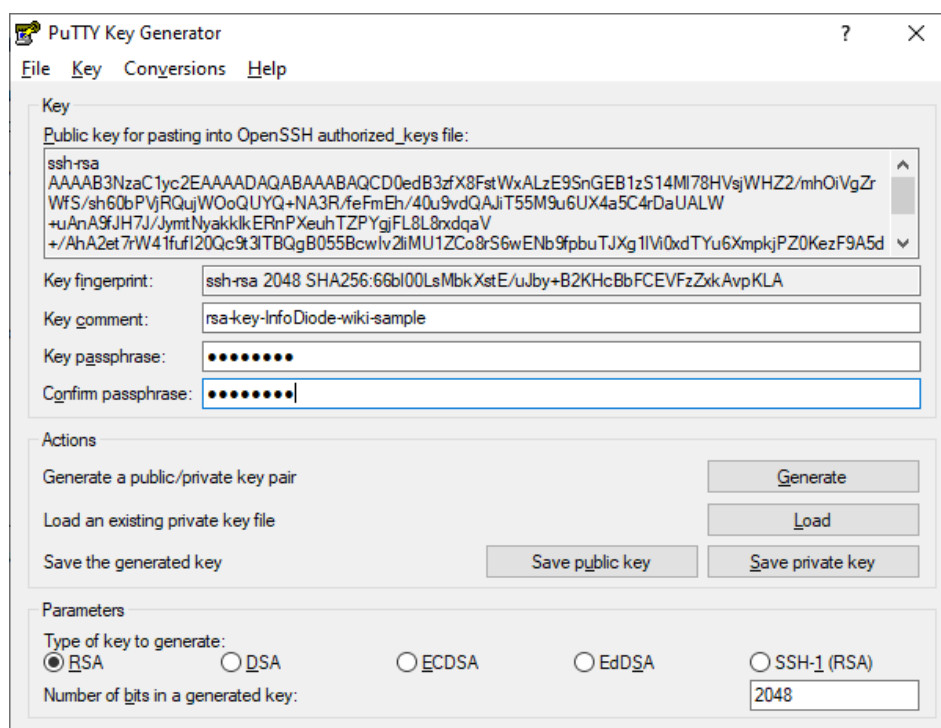
На [странице загрузки](#) PuTTY выбрать архив для необходимой платформы, загрузить его. Для работы в среде Windows наиболее универсальным вариантом будет архив putty.zip

для платформы "32-bit x86". Скачанный архив необходимо распаковать в заранее созданную на флэш-диске папку PuTTY.

4.6.2 Генерация ключей, задание пароля для закрытого ключа

Для генерации пары ключей (закрытый (или приватный, секретный) и открытый (или публичный)) использована утилита PUTTYGEN из состава пакета PuTTY. После запуска PUTTYGEN необходимо нажать кнопку "Generate", после чего перемещать указатель мыши в пустой области "Key" окна программы. Координаты указателя мыши при перемещении используются программой для получения случайных значений в процессе генерации ключей.

По окончании генерации можно изменить комментарий для хранения в файле ключа и задать пароль для ключа в соответствующих полях:



Далее необходимо сохранить закрытый ключ в файл на флэш-диске с PuTTY, например, с именем Infodiode_rsa.ppk.

4.6.3 Перенос открытого ключа на сервер

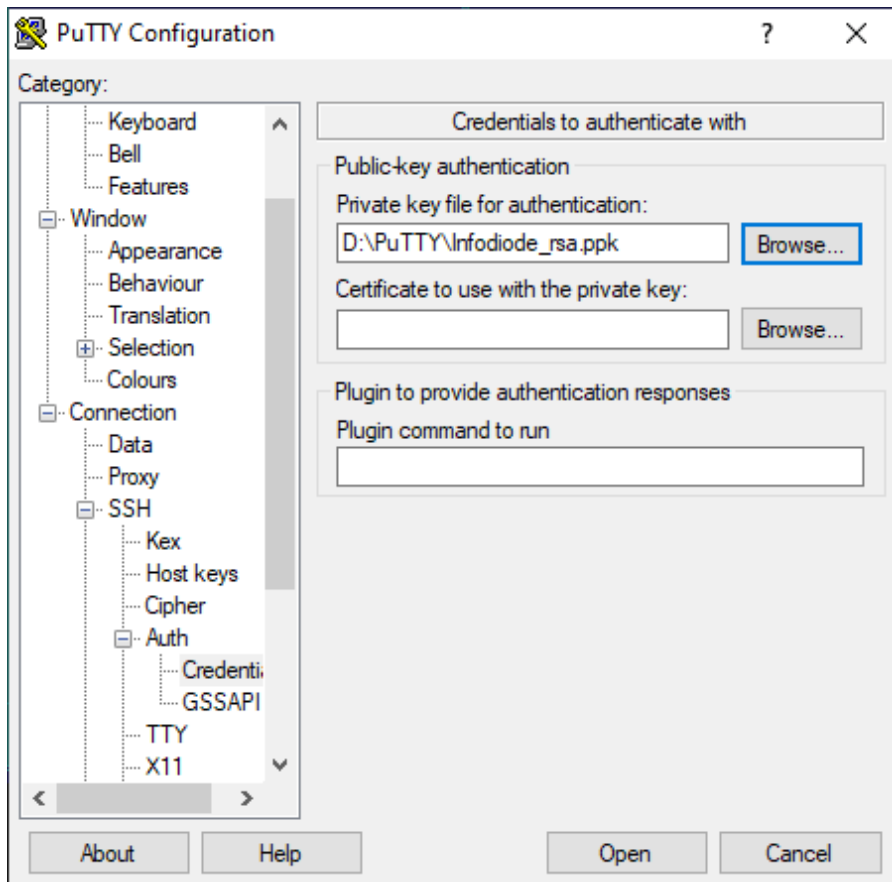
При использования сгенерированного ключа для аутентификации его публичная часть должна быть добавлена в специальный файл ~/.ssh/authorized_keys. Чтобы проделать это, следует подключиться по ssh к выбранному серверу, например, используя PuTTY, авторизоваться под аккаунтом пользователя, для которого необходимо настроить двухфакторную аутентификацию.

Затем выполнить следующие команды, где вместо *PUBKEY* необходимо вставить текст, скопированный из окна "Public key for pasting into OpenSSH authorized_keys file", см. рисунок выше:

```
mkdir -p ~/.ssh
echo *PUBKEY* >> ~/.ssh/authorized_keys
```

4.6.4 Настройка PuTTY для аутентификации с помощью ключа

Чтобы PuTTY при подключении использовала сгенерированный ключ, необходимо указать файл закрытого ключа в настройках подключения, см. рисунок:



4.6.5 Подключение к серверу с использованием ключа и пароля

После запуска PuTTY, выполнения необходимых настроек подключения (или загрузки ранее сохраненных настроек), если предыдущие шаги были выполнены правильно — при подключении пользователь увидит запрос на ввод пароля ключа, например:

```
Using username "diode".
Authenticating with public key "rsa-key-InfoDiode-wiki-sample"
Passphrase for key "rsa-key-InfoDiode-wiki-sample":
```

При ошибке ввода пароля будет выдано сообщение об ошибке "Wrong passphrase" и предложение повторить ввод пароля.

При корректном вводе пользователь будет успешно авторизован.

4.6.6 Изменение пароля ключа

Для изменения пароля необходимо запустить программу PUTTYGEN, загрузить ранее сгенерированный файл ключа (*.ppk), отредактировать пароль, сохранить обновленную версию закрытого ключа. Изменение пароля ключа не требует изменения открытой части ключа на сервере.

4.6.7 Изменение настроек InfoDiode SMART для запрета аутентификации с использованием пароля

Чтобы аутентификация пользователей была возможна только с помощью ключа, необходимо в настройках InfoDiode SMART запретить аутентификацию по паролю. Для этого необходимо создать дополнительный файл настроек сервиса ssh:

/etc/ssh/sshd_config.d/disable-password-auth.conf

```
# Запретить аутентификацию пользователей по паролю
PasswordAuthentication no
```

после чего перезапустить сервис ssh. Внесенные изменения запретят аутентификацию по паролю для всех пользователей.

Если для некоторых пользователей (или групп пользователей, или хостов/адресов) есть необходимость использовать особые настройки, отличающиеся от глобальных — можно использовать настройки внутри условного блока (подробности по ссылке [man sshd_config](#)). Например, ниже показаны настройки, разрешающие использование пароля для аутентификации пользователей plainuser и justuser, а также при подключении с любого хоста из доверенной подсети с адресами 192.168.33.*:

/etc/ssh/sshd_config.d/password-auth.conf

```
# Запретить аутентификацию пользователей по паролю
PasswordAuthentication no
# Использование пароля для аутентификации пользователей plainuser и justuser
разрешено
Match User plainuser,justuser
    PasswordAuthentication yes
# Использование пароля для аутентификации при подключении с любого хоста из
доверенной подсети с адресами 192.168.33.* разрешено
Match Address 192.168.33.0/24
    PasswordAuthentication yes
```

Все строки после строки начала условного блока "Match" считаются относящимися к этому блоку, поэтому блоки "Match" размещаются в конце файла настроек

Не следует редактировать файл `/etc/ssh/sshd_config`, он поддерживается разработчиками и может измениться при обновлении ОС в будущем.

Вместо редактирования `/etc/ssh/sshd_config` можно создавать дополнительные файлы настроек `/etc/ssh/sshd_config.d/*.conf`. Эти настройки являются приоритетными.

4.7 Отключение доступа по SSH

АПК InfoDiode SMART light поставляется с разрешённым доступом по SSH для всех пользователей, кроме `root'a`, при необходимости его отключить, следует выполнить команду:

Команду можно выполнить в локальной сессии или в SSH сессии, в таком случае текущая сессия останется активной, но не будет возможно открыть новые SSH сессии

```
systemctl disable --now ssh.service
```

Если необходимо снова разрешить доступ по SSH выполните команду:

```
systemctl enable --now ssh.service
```

5. Настройка системных сервисов

5.1 Настройка брандмауэра

АПК InfoDiode SMART light поставляется с предварительно настроенным брандмауэром.

Сетевые интерфейсы привязаны к следующим зонам `firewalld`:

`data` —> `data`

`diode-in`, `diode-out` —> `diode-link`

По умолчанию: в АПК InfoDiode SMART light разрешены входящие соединения со всех сетевых адресов по порту 22 (SSH).

Для изменения настроек необходимо использовать команду `firewall-cmd`, для того что бы применить изменения необходимо перезагрузить `firewalld` с помощью команды `firewall-cmd --reload`.

Документация по использованию команды `firewall-cmd`:

<https://firewalld.org/documentation/man-pages/firewall-cmd>

После применения конфигурации проверьте статус сервиса `firewalld` с помощью команды:

```
systemctl status firewalld.service
```

5.2 Конфигурирование NTP и параметров таймзоны

АПК InfoDiode SMART light поставляется с отключенной синхронизацией по NTP. При необходимости ее активировать, следует:

- Выполнить команду:

```
systemctl enable --now systemd-timesyncd.service
```

- Указать в файле `/etc/systemd/network/10-data.network` в секции `[Network]` NTP сервер для синхронизации, например, `NTP=pool.ntp.org`;
- Активировать синхронизацию по NTP командой

```
timedatectl set-ntp 1
```

- Перезагрузить узел.

Для отключения синхронизации

- В файле `/etc/systemd/network/10-data.network` в секции `[Network]` удалить строку, задающую NTP сервер для синхронизации, например, `NTP=pool.ntp.org`;
- Выполнить команду

```
timedatectl set-ntp 0
```

- Выполнить команду:

```
systemctl disable --now systemd-timesyncd.service
```

- Перезагрузить узел.

АПК InfoDiode SMART light поставляется с заданной таймзоной `Europe/Moscow`. При необходимости задать местную таймзону следует использовать команду:

```
timedatectl set-timezone <таймзона>
```

, например:

```
timedatectl set-timezone Europe/Moscow
```

для вывода списка зон следует использовать команду:

```
timedatectl list-timezones
```

Для корректного применения настроек необходимо перезагрузить узел с помощью команды `reboot`.

5.3 Настройка сервиса мониторинга

PLANNED

6. Настройка коннекторов

В составе АПК InfoDiode SMART light поставляются коннектор FILE <-> MQTT (UDP) и коннектор Modbus <-> MQTT (UDP).

Важно учитывать, что в АПК InfoDiode SMART light используется только UDP передача для коннекторов, поэтому в `{file,modbus}-common.protocol` необходимо указывать протокол UDP, а так же:

1. На IN-части в конфигурации коннекторов для параметра `udp-transmitter.host` необходимо указывать `192.168.255.254`
2. На OUT-части в конфигурации коннекторов для параметра `udp-receiver.host` необходимо указывать `192.168.255.253`

При их настройке необходимо руководствоваться соответствующими инструкциями, сервисы по умолчанию выключены и нуждаются в дополнительной настройке:

1. [Коннектор FILE <-> MQTT\(UDP\)](#)
 1. Важно учитывать, что в составе АПК InfoDiode SMART light уже включены пакеты `vsftpd` и `samba` для работы по протоколам FTP/SMB, их необходимо включить и разрешить в `firewalld`, открыв соответствующие порты.
2. [Коннектор Modbus <-> MQTT \(UDP\)](#)

7. Мониторинг, диагностика, контроль состояния

7.1 Просмотр событий при доступе через SSH / Serial

В качестве реализации механизма системного журнала, используется решение [systemd-journal](#).

При работе с командной строкой, для просмотра содержимого системного журнала используется утилита `journalctl`. Наиболее часто используемые опции:

Опция	Описание	Пример использования	Комментарий к примеру
Фильтрация			

-b <N>	Просмотр содержимого журнала N-й загрузки системы, где N — 0 для текущей загрузки, -1 — предыдущая загрузка, -2 — пред-предыдущая загрузка и т. д.	journalctl -b	С момента последнего запуска.
		journalctl -b -2	Пред-предыдущая загрузка.
-n <N>	Вывод последних N записей журнала.	journalctl -n 100	Вывод последних 100 записей.
-p <P>	Отфильтровать сообщения, имеющие указанный или более высокий приоритет: • emerg (0) • alert (1) • crit (2) • err (3) • warning (4) • notice (5) • info (6) • debug (7)	journalctl -p err	Вывод сообщений с приоритетом err и выше.
-k	Просмотр содержимого журнала ядра системы.	journalctl -k	
-u <unit>	Просмотр содержимого журнала конкретной службы (unit'a).	journalctl -u idsmart-core	Просмотр записей Ядра ПО.
Параметры вывода			
--no-hostname	Не выводить имя сервера.	journalctl --no-hostname	
-f	Вывод сообщений в режиме реального времени.	journalctl -f	

<code>-o</code> <code><format></code>	Использовать определенный формат вывода. Рекомендуемые основные: • <code>short-precise</code> — вывод с дополнительной точностью по времени • <code>export</code> — формат для экспорта записей журнала • <code>json</code> — вывод в формате <code>json</code> • <code>json-pretty</code> — вывод в формате <code>json</code> с форматированием	<code>journalctl -o json-pretty</code>	
--	--	--	--

Пример:

- просмотр всех событий системы с момента последнего запуска:

```
journalctl --no-hostname -b
```

- просмотр всех событий Ядра ПО уровня `err` и выше с момента последнего запуска:

```
journalctl --no-hostname -b -u idsmart-core -p err
```

- запуск мониторинга журнала Ядра ПО в режиме реального времени:

```
journalctl --no-hostname -u idsmart-core -f
```

По умолчанию, при запуске через **SSH** или **Serial**, **journalctl** осуществляет постраничный вывод с навигацией (аналогично вызову утилиты **less**). Данное поведение может быть отключено передачей опции `--no-pager`.

Детальная информация по параметрам вызова может быть получена следующей командой: `journalctl --help`

7.2 Передача данных журнала на внешний сервер по протоколу syslog

Передача данных журнала по протоколу Syslog осуществляется с помощью ПО `rsyslog`. Файл конфигурации со списком адресов для отправки журналов располагается по пути `/etc/rsyslog.d/rsyslog.local.conf`. Строки в данном файле записываются в формате: `<фильтр> <назначение>`, где:

- <фильтр> — одна или более записей вида <facility>.<level>, перечисленных через точку с запятой:
 - <facility> — код syslog системной службы - или * в случае, если фильтровать по facility не требуется
 - <level> — минимальный уровень
- <назначение> — адрес доставки записей журнала в формате <протокол><адрес>:<порт>:
 - <протокол> — необходимо указать @ для UDP и @@ для TCP
 - <адрес> — IP-адрес syslog-коллектора
 - <порт> — порт syslog-коллектора

Пример файла конфигурации /etc/rsyslog.d/rsyslog.local.conf:

```
# Все записи с уровнем info и выше отправляются на 10.0.144.101.
*.info @10.0.0.1:514
# Все записи
*.* @@10.0.0.2:514
```

После изменения файла требуется применить конфигурацию сервиса rsyslog командой:
systemctl restart rsyslog.service

8.Обновление пакетов ОС и ПО коннекторов

8.1 Обновление пакетов ОС

При поставке сетевые репозитории apt в файле /etc/apt/sources.list
закомментированы и отсутствуют DNS в файле конфигурации
/etc/systemd/network/10-data.network.

Если требуется обновить пакеты и ПО, то необходимо раскомментировать сетевые
репозитории apt в файле /etc/apt/sources.list и настроить DNS, после чего можно
выполнить apt update.

8.2 Обновление коннекторов

При обновлении коннекторов следует руководствоваться инструкциями на
соответствующий тип коннекторов.