



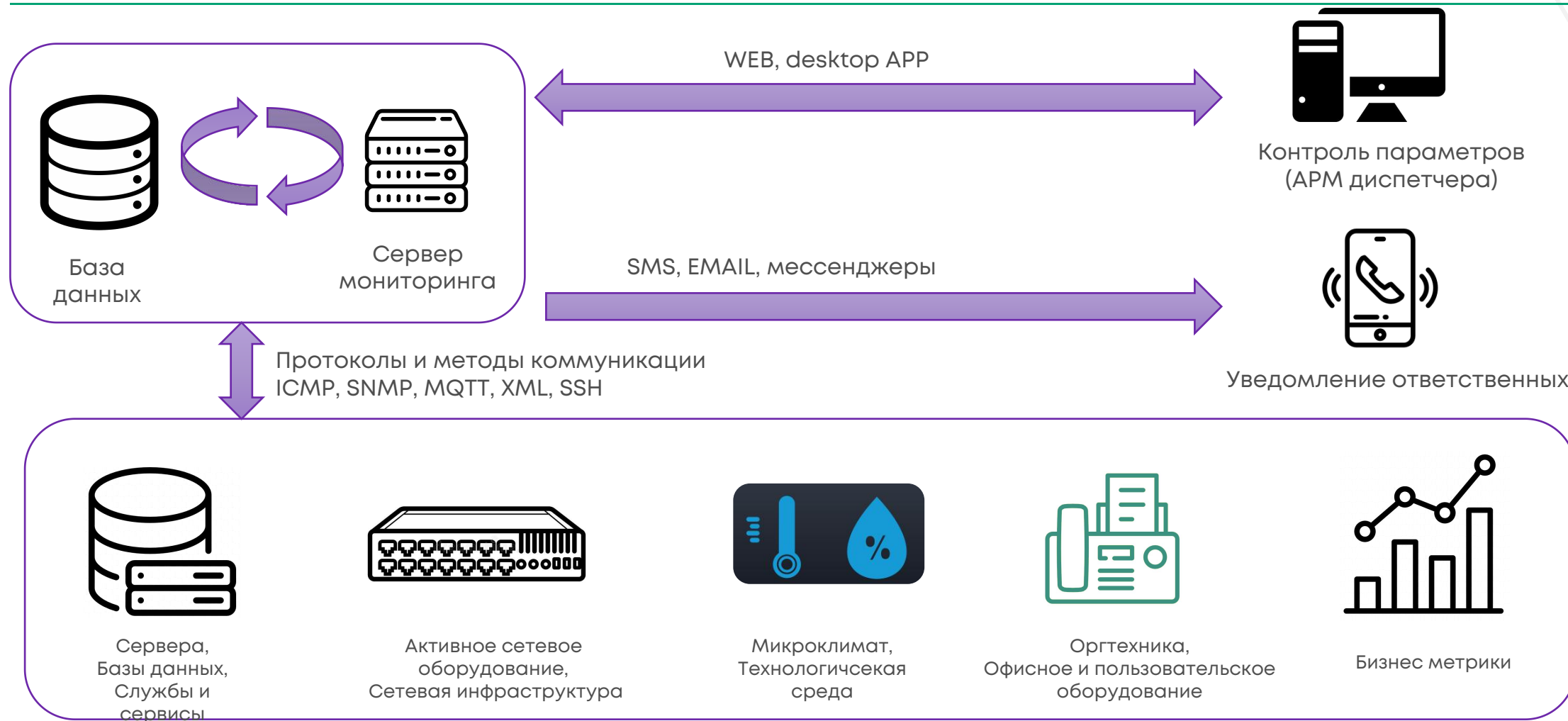
nag[®]
Следуй за экспертом

Интеграция в систему мониторинга устройств SNR-ERD по средствам SNMP

- Мониторинг - это комплекс процессов непрерывного наблюдения за явлениями, событиями и состоянием отдельных параметров, в рамках наблюдаемой системы, с целью эффективного управления и обоснования управленческих решений
- Мониторинг ИТ-инфраструктуры - это процесс автоматического контроля и своевременного информирования, который позволяет отслеживать параметры ИТ-инфраструктуры, работоспособность сети, состояние окружающей и технологической среды в местах размещения оборудования
- Система мониторинга - это инструмент непрерывного анализа контролируемой инфраструктуры и протекающих в ней процессов.

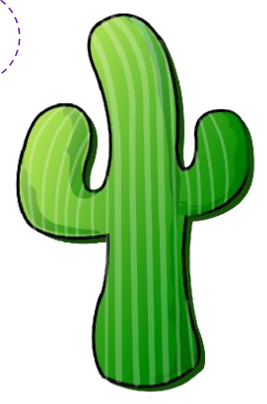


Структурная схема мониторинга ИТ-инфраструктуры





1



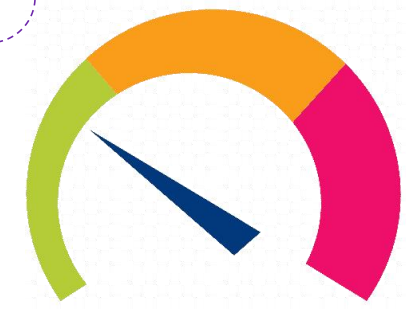
2



3



4



5



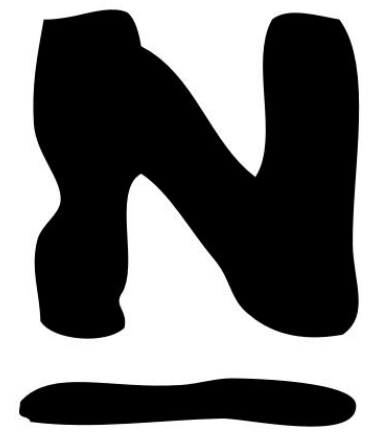
6



7



8

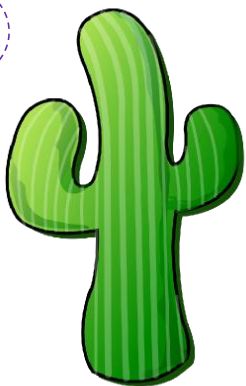


9



Системы мониторинга

1



Cacti
(41голос)

2



Zabbix
(157 голосов)

3



Glaber
(1 голос)

4



PRTG
(9 голосов)

5



Observium
(21 голос)

6



LibreNMS
(16 голосов)

7



Prometheus
(13 голосов)

8



Nagios
(18 голосов)

9



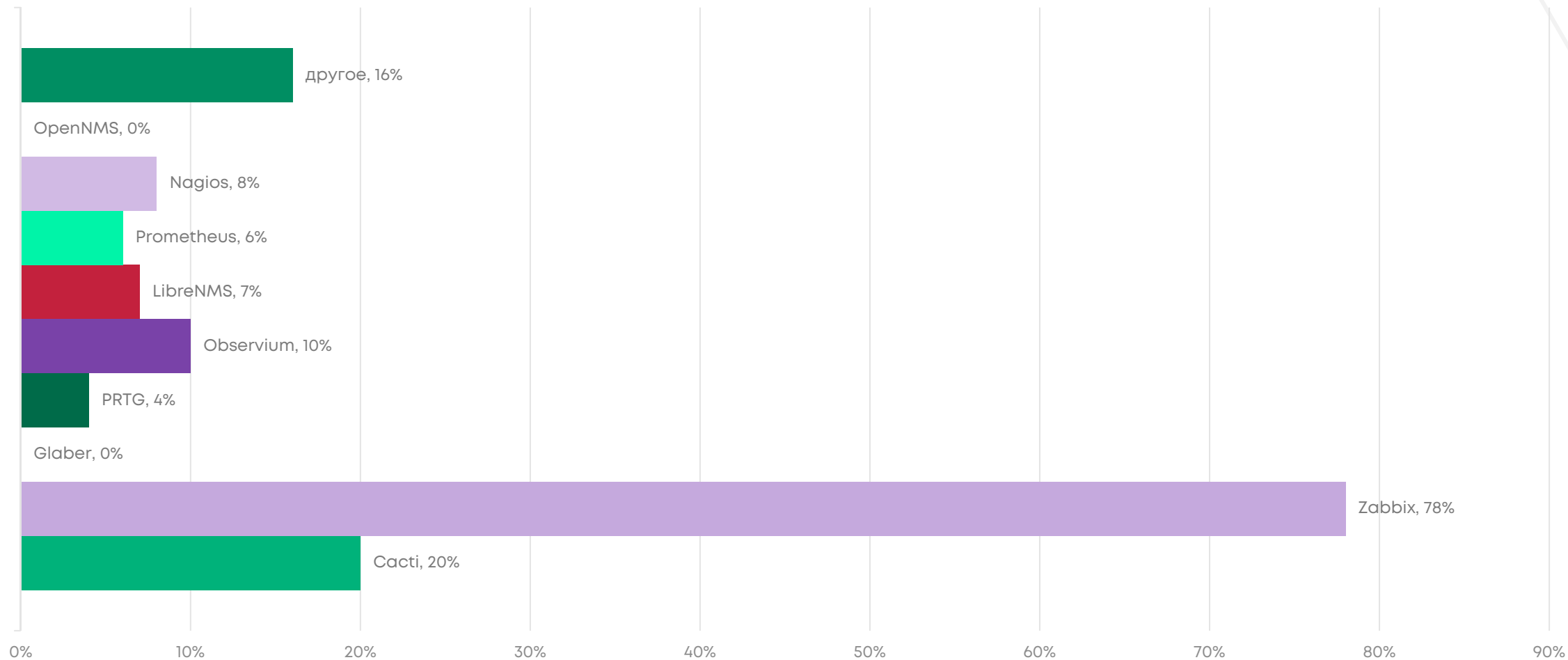
OpenNMS
(2 голоса)



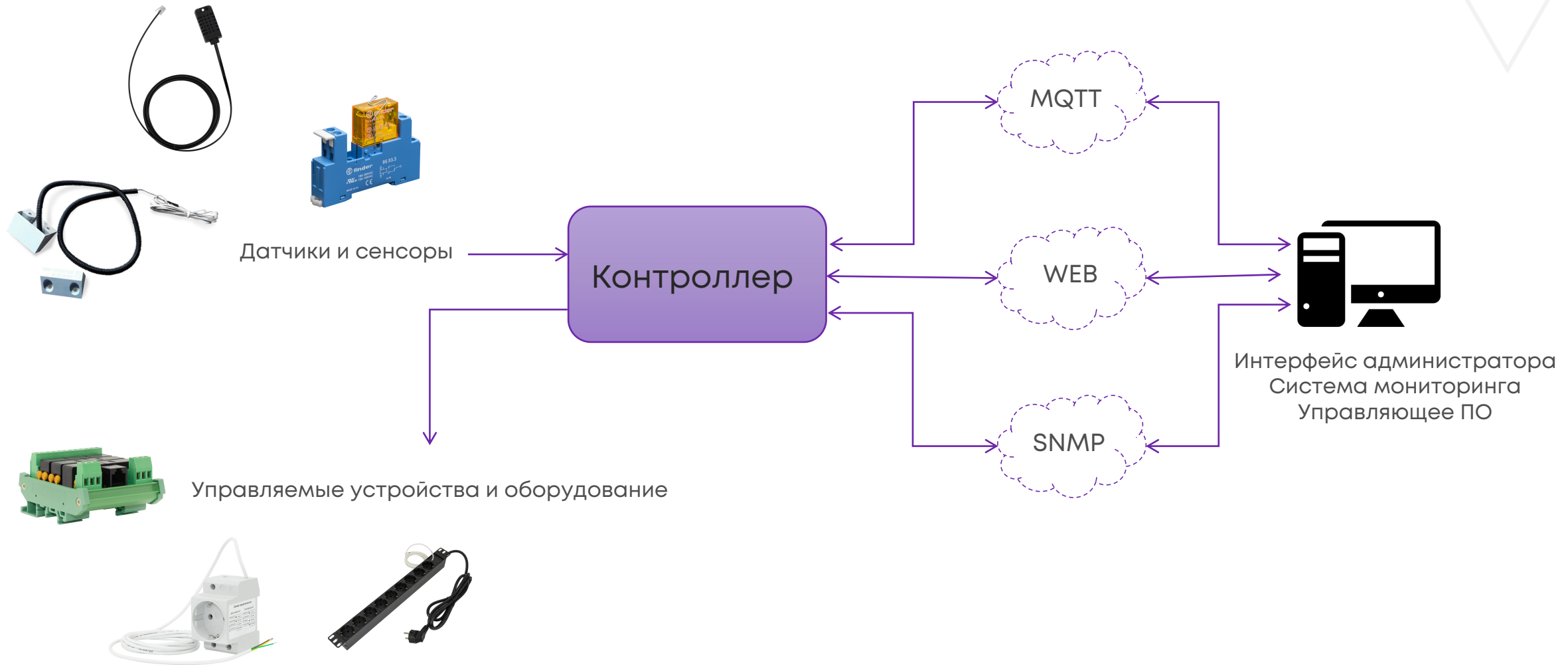
Всего: 312 голосов

Другое (34 голоса)

Самые используемые системы мониторинга



Оборудование для организации мониторинга технологических параметров



Контроллеры SNR. SNR-ERD-2XX



ERD-2s



ERD-2.3



ERD-2.3-DHT22



ERD-2.3-termo-out

Контроллеры SNR. SNR-ERD-4s/SNR-ERD-4s-GSM



ERD-4s



ERD-4s-GSM

Контроллеры SNR. SNR-ERD-5c



ERD-5c

Контроллеры SNR. SNR-SNMP-CARD-801



SNMP-CARD-801

Сравнительная таблица. Аппаратный функционал



	ERD-2.3/thermo-out/DHT22	ERD-2s	ERD-4s/GSM	ERD-5c	SNMP-CARD-801
Тип корпуса	Термоусадка	Металл	Металл	Термоусадка	-
Питание	DC 5V	DC 9-48V	DC 9-48V	DC 9-36V	От UPS
Поддержка PoE	-	+	+	-	-
Ethernet порт	10Mb/s HALF duplex	10Mb/s HALF duplex	100Mb/s FULL duplex	100Mb/s FULL duplex	100Mb/s FULL duplex
DIO	2DO (I _{max} =300mA) 3DI	2DO (I _{max} =200mA) 4DI	5DIO (I _{max} =200mA)	5DIO (I _{max} =10mA) 1DIO (I _{max} =200mA)	2DIO (I _{max} =200mA)
Датчик фазы	DC 5V (jack)	DC 5V (клеммы)	DC 5V (клеммы)	AC220V	-
Последовательный интерфейс RS-485/232	-	-	+	+	-
Порты для питания внешних устройств	3V3/100mA 5V/200mA	3V3/100mA 5V/200mA	5V/до 2500mA 12V/100mA	5V/до 2500mA 9-36V (дублирует источник питания)	-
Аналоговый выход (DAC)	-	-	+	-	-
Аналоговый вход (ADC) (0-76V)	1шт	1шт	1шт	2шт	-
Встроенное реле	-	-	+	-	-

Сравнительная таблица. Программный функционал



	ERD-2.3/termo-out/DHT22	ERD-2s	ERD-4s/GSM	ERD-5c	SNMP-CARD-801
GSM функционал	-	-	+ (в GSM версии)	-	-
Поддержка 1-wire	+ (кроме DHT22)	+	+	+	+
Сетевая диагностика (watchdog)	+	+	+	+	+
ПИД-регулятор	-	-	+	-	-
Термостат/Гидролок	+	+	+	-	+
Мониторинг параметров UPS	-	-	+	+	+
DHCP	-	-	+	+	+
SNMP	v1	v1	v2c v3	v2c	v2c
MQTT	-	-	+	-	-
Конфигурация чтение/запись	-	-	+	+	+
Журнал событий	-	-	+	-	+

SNMP (~~Security is Not My Problem~~) (Simple Network Management Protocol)



«Простой» протокол сетевого управления

Обсуждение:

1. Используете ли Вы SNMP?
2. Какие устройства опрашиваете по SNMP?
3. Какое серверное ПО используете для опроса?
4. Какие утилиты используете?
5. Что такое MIB?



SNMP возглавляет составленный SANS Institute список «Common Default Configuration Issues» с вопросом изначальной установки строк сообщества на значения «public» и «private» и занимал десятую позицию в SANS Top 10 Самых критических угроз Интернет-безопасности за 2000 год.



- RFC1155 (STD 16) — Structure and Identification of Management Information for the TCP/IP-based Internets
- RFC1156 (Historic) — Management Information Base for Network Management of TCP/IP-based internets
- RFC1157 (Historic) — A Simple Network Management Protocol (SNMP)
- RFC1213 (STD 17) — Management Information Base for Network Management of TCP/IP-based internets: MIB-II
- RFC1452 (Informational) — Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework
- RFC1901 (Experimental) — Introduction to Community-based SNMPv2
- RFC1902 (Draft Standard) — Structure of Management Information for SNMPv2
- RFC1908 (Standards Track) — Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
- RFC2570 (Informational) — Introduction to Version 3 of the Internet-standard Network Management Framework
- RFC2578 (STD 58) — Structure of Management Information Version 2 (SMIv2)
- RFC3410 (Informational) — Introduction and Applicability Statements for Internet Standard Management Framework
- STD62 contains the following RFCs:
 - RFC3411 — An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
 - RFC3412 — Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
 - RFC3413 — Simple Network Management Protocol (SNMP) Applications
 - RFC3414 — User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
 - RFC3415 — View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
 - RFC3416 — Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
 - RFC3417 — Transport Mappings for the Simple Network Management Protocol (SNMP)
 - RFC3418 — Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC3430 (Experimental) — Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping
- RFC3584 (BCP 74) — Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
- RFC3826 (Proposed) — The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC4789 (Proposed) — Simple Network Management Protocol (SNMP) over IEEE 802 Networks
- RFC5343 (STD 78) — Simple Network Management Protocol (SNMP) Context EngineID Discovery
- RFC5590 (STD 78) — Transport Subsystem for the Simple Network Management Protocol (SNMP)
- RFC5591 (STD 78) — Transport Security Model for the Simple Network Management Protocol (SNMP)
- RFC5592 (Proposed) — Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)
- RFC5608 (Proposed) — Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models.
- RFC6353 (STD 78) — Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)
- RFC7630 (Proposed) — HMAC-SHA-2 Authentication Protocols in the User-based Security Model (USM) for SNMPv3

Команды snmpget , snmpset, snmpwalk, snmptable

```
snmpwalk -v3 -l 'authNoPriv' -n '' -a 'MD5' -A 'academy.nag.ru' -u 'observium' erd4-lab.nag.ru:55161 .1.3.6.1.4.1.40418.2.6.2.1.1
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.1.3 = STRING: "DIO3"
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.1.4 = STRING: "DIO4"
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.1.5 = STRING: "DIO5"
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.1.6 = STRING: "PhaseSensor"
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.3.1.3 = INTEGER: 1
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.3.1.4 = INTEGER: 1
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.3.1.5 = INTEGER: 1
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.3.1.6 = INTEGER: 1
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.4.1.3 = Counter32: 0
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.4.1.4 = Counter32: 0
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.4.1.5 = Counter32: 0
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.4.1.6 = Counter32: 0
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.5.1.3 = INTEGER: 0
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.5.1.4 = INTEGER: 0
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.5.1.5 = INTEGER: 0
```

```
iso.3.6.1.4.1.40418.2.6.2.1.1.5.1.6 = INTEGER: 0
```


Практическая работа. Знакомство с ERD



ERD-4s



PHD-DIN-1.0



ERD-2.3-DHT22



SMART-DIN-A



DTS-2



DOOR SENSOR
SNR-DS-01



DHTS-0.5m

Методические материалы находятся по ссылке: <https://data.nag.wiki/SNR%20ERD/Academy2023/>

Система мониторинга Observium

<http://observium.org>

https://www.observium.org/supported_devices/

<http://192.168.15.197/> / <http://o.nag.mtik.pro>





Логин: user<XY>

Пароль: academyNAG2023

/etc/hosts:

- erd-<XY>.academy.nag.ru -> 192.168.15.<XY>
- erd4-<XY>.academy.nag.ru -> 192.168.15.2<XY>

Devices -> Add device



./discovery.php -h 7 -m sensors

```
Observium
Observium Professional 23.10.13038
https://www.observium.org

#### Starting discovery run at 2023-10-09 04:15:14 ####

#### erd4-lab.nag.ru [7] ####

o OS Type          snr-erd
o OS Group         environment
o SNMP Version     v3
o Last discovery   2023-10-09 04:14:50
o Last duration    1.54 seconds

#### Module Start: sensors ####

o SNR-ERD-4        adcSensor [.] temperatureDHT [] humidityDHT [] rsshTemp [.] rsshHum
[.] rsshPssr [.] rsshPlWTemp [.....] dtsTemp [] gsmStrength [.] gsmReconnCount [.]
o SNR-ERD-4        diState [.....] doState [.] connectStatusRS485 [.] connectStatusR
S232 [.] statusUPS []
o ENTITY-SENSOR-MIB

o Duration         2.0262s
```



```
./discovery.php -h 7 -m sensors -dd
```

```
o SNR-ERD-4          diState [  
CMD[/usr/bin/snmpbulkwalk -v3 -l 'authNoPriv' -n '' -a 'MD5' -A 'academy.nag.ru' -u 'observium'  
-Pud -Ih -OQusb -m SNR-ERD-4 -M /opt/observium/mibs/rfc:/opt/observium/mibs/net-snmp:/opt/observ  
ium/mibs/snr 'udp':'erd4-lab.nag.ru':'55161' diEntry]  
  
CMD EXITCODE[0]  
CMD RUNTIME[0.1615s]  
CMD EXITDELAY[5ms]  
STDOUT[  
diName.1.3 = "DI03"  
diName.1.4 = "DI04"  
diName.1.5 = "DI05"  
diName.1.6 = "PhaseSensor"  
diName.2181300500.1 = "Count-LAB2: DI1"  
diName.2181300500.2 = "Count-LAB2: DI2"  
diName.2181300500.3 = "Count-LAB2: DI3"  
diName.2181300500.4 = "Count-LAB2: DI4"  
diName.2181300500.5 = "Count-LAB2: DI5"  
diName.2181300500.6 = "Count-LAB2: DI6"  
diName.2181300500.7 = "Count-LAB2: DI7"  
diName.2181300500.8 = "Count-LAB2: DI8"  
diAlarmName.1.3 = "ALARM-3"  
diAlarmName.1.4 = "ALARM-4"  
diAlarmName.1.5 = "ALARM-5"  
diAlarmName.1.6 = "usense"  
diAlarmName.2181300500.1 = "TEST0"  
diAlarmName.2181300500.2 = "TEST2"  
diAlarmName.2181300500.3 = "TEST3"  
diAlarmName.2181300500.4 = "TEST4"  
diAlarmName.2181300500.5 = "TEST5"  
diAlarmName.2181300500.6 = "TEST6"  
diAlarmName.2181300500.7 = "TEST7"  
diAlarmName.2181300500.8 = "TEST8"  
diState.1.3 = high  
diState.1.4 = high  
diState.1.5 = high  
diState.1.6 = high
```

Команды snmpget , snmpset, snmpwalk, snmptable

```
snmpbulkwalk -v3 -l 'authNoPriv' -a 'MD5' -A 'academy.nag.ru' -u 'observium' -M mibs/rfc:mibs/net-snmp:mibs/snr  
erd4-lab.nag.ru:55161 SNR-ERD-4::diEntry
```

```
SNR-ERD-4::diName.1.3 = STRING: "DIO3"
```

```
SNR-ERD-4::diName.1.4 = STRING: "DIO4"
```

```
SNR-ERD-4::diName.1.5 = STRING: "DIO5"
```

```
SNR-ERD-4::diName.1.6 = STRING: "PhaseSensor"
```

```
SNR-ERD-4::diAlarmName.1.3 = STRING: "ALARM-3"
```

```
SNR-ERD-4::diAlarmName.1.4 = STRING: "ALARM-4"
```

```
SNR-ERD-4::diAlarmName.1.5 = STRING: "ALARM-5"
```

```
SNR-ERD-4::diAlarmName.1.6 = STRING: "usense"
```

```
SNR-ERD-4::diState.1.3 = INTEGER: high(1)
```

```
SNR-ERD-4::diState.1.4 = INTEGER: high(1)
```

```
SNR-ERD-4::diState.1.5 = INTEGER: high(1)
```

```
SNR-ERD-4::diState.1.6 = INTEGER: high(1)
```

```
SNR-ERD-4::diCnt.1.3 = Counter32: 0
```

```
SNR-ERD-4::diCnt.1.4 = Counter32: 0
```

```
SNR-ERD-4::diCnt.1.5 = Counter32: 0
```

```
SNR-ERD-4::diCnt.1.6 = Counter32: 0
```

```
snmptable ... diTable
```

```
SNMP table: SNR-ERD-4::diTable
```

diName	diAlarmName	diState	diCnt
"DIO3"	"ALARM-3"	high	0
"DIO4"	"ALARM-4"	high	0
"DIO5"	"ALARM-5"	high	0
"PhaseSensor"	"usense"	high	0
"Count-LAB2: DI1"	"TEST0"	high	6
"Count-LAB2: DI2"	"TEST2"	low	0
"Count-LAB2: DI3"	"TEST3"	high	0
"Count-LAB2: DI4"	"TEST4"	low	0
"Count-LAB2: DI5"	"TEST5"	high	0
"Count-LAB2: DI6"	"TEST6"	low	0
"Count-LAB2: DI7"	"TEST7"	high	0
"Count-LAB2: DI8"	"TEST8"	low	9

Команды snmpget , snmpset, snmpwalk, snmptable

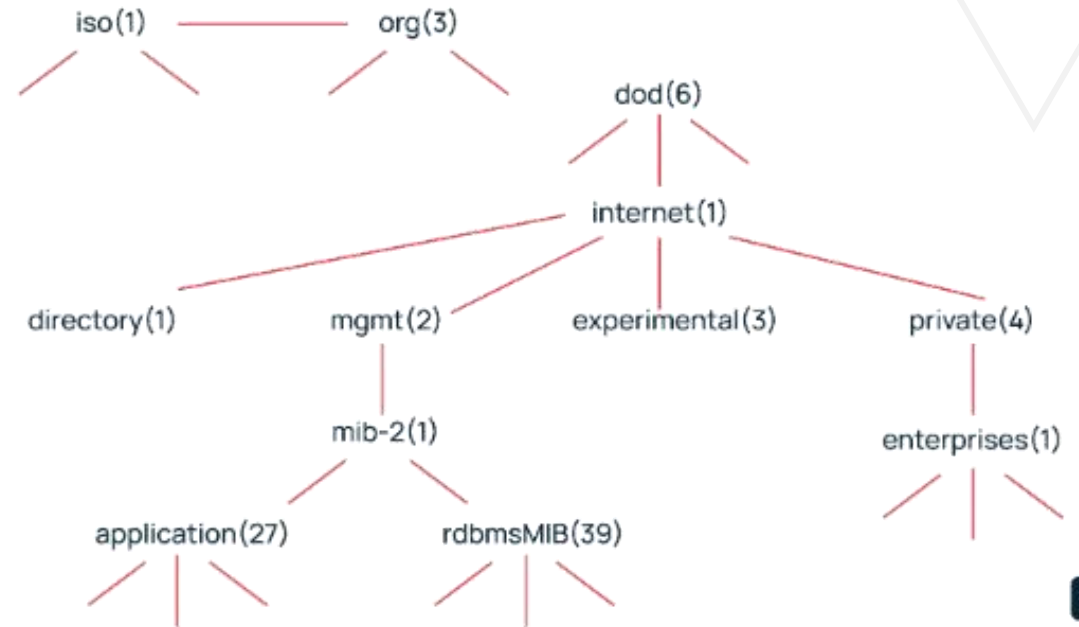
```
snmpget -v3 <...> erd4-lab.nag.ru:55161 \  
.1.3.6.1.4.1.40418.2.6.1.2.0 .1.3.6.1.4.1.40418.2.6.5.1.2.0 \  
.1.3.6.1.4.1.40418.2.6.1.30.100.1.3.441839376
```

Без MIB

```
iso.3.6.1.4.1.40418.2.6.1.2.0 = INTEGER: 0  
iso.3.6.1.4.1.40418.2.6.1.30.100.1.3.441839376 = INTEGER: 23  
iso.3.6.1.4.1.40418.2.6.5.1.2.0 = INTEGER: -89
```

Стандартные MIB (-m RFC1155-SMI)

```
RFC1155-SMI::enterprises.40418.2.6.1.2.0 = INTEGER: 0  
RFC1155-SMI::enterprises.40418.2.6.1.30.100.1.3.441839376 = INTEGER: 23  
RFC1155-SMI::enterprises.40418.2.6.5.1.2.0 = INTEGER: -89
```



Команды snmpget , snmpset, snmpwalk, snmptable

```
snmpget -v3 <...> erd4-lab.nag.ru:55161 \
```

```
.1.3.6.1.4.1.40418.2.6.1.2.0 .1.3.6.1.4.1.40418.2.6.5.1.2.0 \
```

```
.1.3.6.1.4.1.40418.2.6.1.30.100.1.3.441839376
```

Без MIB

```
iso.3.6.1.4.1.40418.2.6.1.2.0 = INTEGER: 0
```

```
iso.3.6.1.4.1.40418.2.6.1.30.100.1.3.441839376 = INTEGER: 23
```

```
iso.3.6.1.4.1.40418.2.6.5.1.2.0 = INTEGER: -89
```

Стандартные MIB (-m RFC1155-SMI)

```
RFC1155-SMI::enterprises.40418.2.6.1.2.0 = INTEGER: 0
```

```
RFC1155-SMI::enterprises.40418.2.6.1.30.100.1.3.441839376 = INTEGER: 23
```

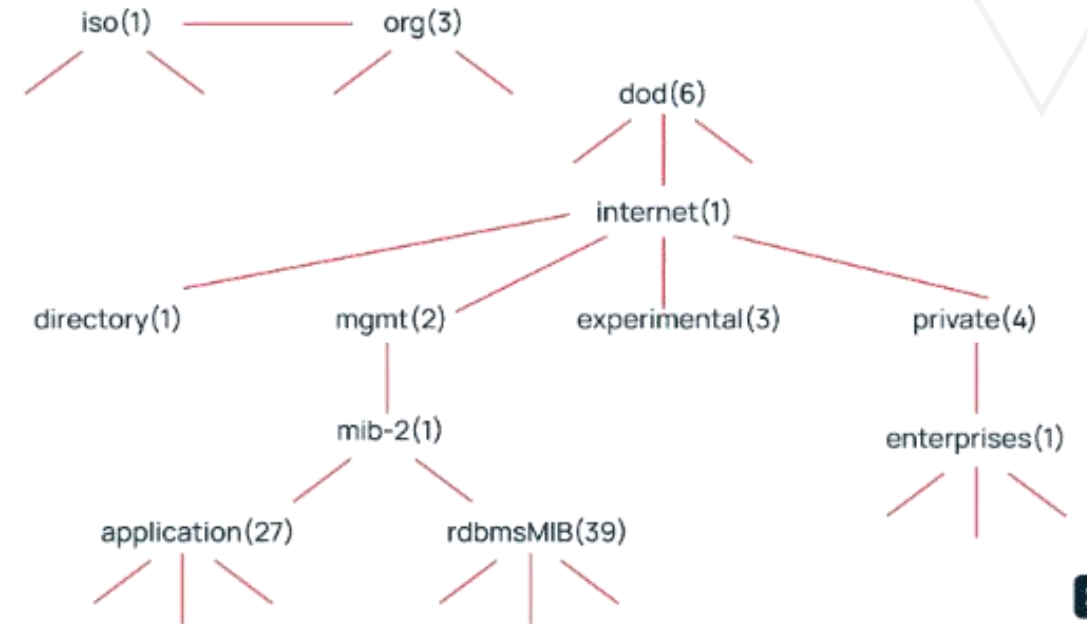
```
RFC1155-SMI::enterprises.40418.2.6.5.1.2.0 = INTEGER: -89
```

С проприетарным MIB (-m SNR-ERD-4)

```
SNR-ERD-4::adcSensor.0 = INTEGER: 0 Volt DC
```

```
SNR-ERD-4::rsshttp1WTemp.441839376 = INTEGER: 23 degrees Centigrade
```

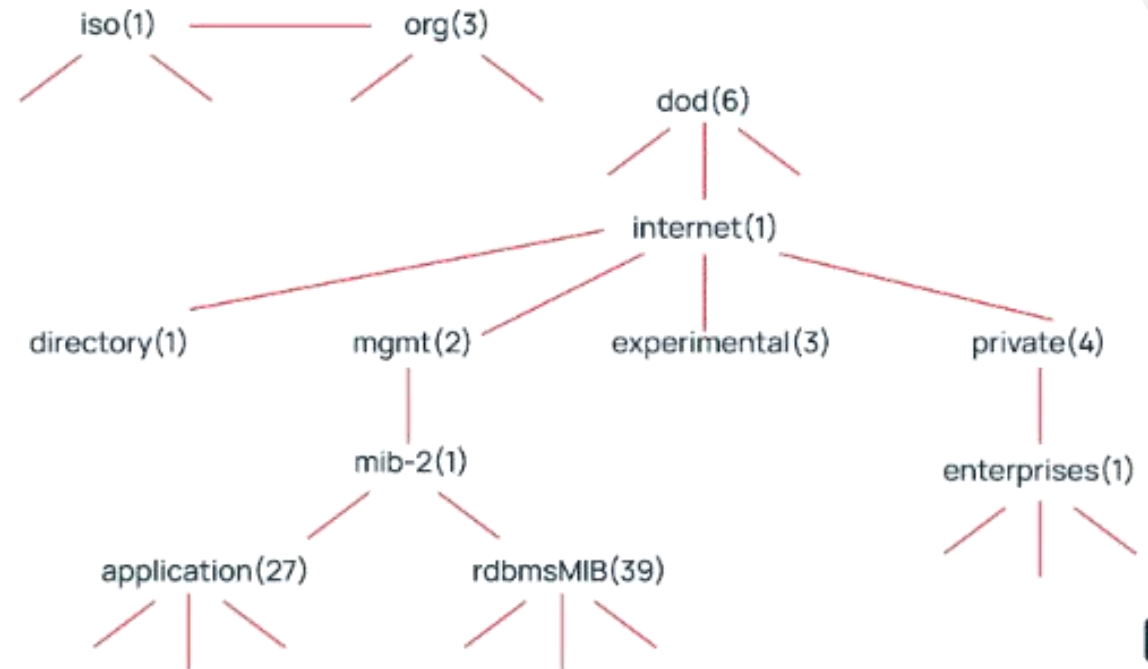
```
SNR-ERD-4::gsmStrength.0 = INTEGER: -89 dBm
```



SNMP – структура MIB

```
snmptranslate -Tp -M mibs:mibs/rfc:mibs/net-snmp:mibs/snr -m SNR-ERD-4 \  
.1.3.6.1.4.1.40418.2.6.1.2.0 \  
.1.3.6.1.4.1.40418.2.6.5.1.2.0 \  
.1.3.6.1.4.1.40418.2.6.1.30.100.1.3.441839376
```

```
+--snr(40418)  
  +--snr-erd(2)  
    +--snr-erd-4(6)  
      +--measurements(1)  
        | +-- -R-- Integer32 adcSensor(2)  
        | +--sp(30)  
        |   +--rssh1WTable(100)  
        |     +--rssh1WEntry(1)  
        |       | Index: rssh1WIdent  
        |       +-- -R-- Unsigned rssh1WIdent(1)  
        |         | Textual Convention: SensorID  
        |         | Range: 0..4294967295  
        |         +-- -RW- String rssh1WName(2)  
        |         +-- -R-- Integer32 rssh1WTemp(3)  
      +--modules(5)  
        | +--gsm(1)  
        |   |  
        |   +-- -R-- EnumVal gsmModuleStatus(1)  
        |     | Values: No(0), Yes(1), NoSim(2), Error(3), Connected(4)  
        |     +-- -R-- INTEGER gsmStrength(2)
```



SNMPv1 — Community-based security

Первая версия протокола создана в 80-х годах XX века. Легка в настройке — требуется только строка community.

SNMPv2c — Community-based security

Вторая версия протокола SNMP появилась в 1993 году.

Добавили:

- запрос GetBulk и ловушку Inform
- 64-bit counters
- усовершенствовали безопасность.

SNMPv3 — User-based security

Третья версия вышла в 1998 году.

Добавили:

- Аутентификацию
- Конфиденциальность
- Целостность
- Контексты

SNMP: Protocol Data Unit (PDU)

GET — запрос менеджера NMS на получение данных с устройства.

GETNEXT — запрос, аналогичный GET. Отличие лишь в том, что менеджер запрашивает данные, находящиеся на следующем уровне иерархии OID, в MIB.

GETBULK — запрос агенту на извлечение с устройства массива данных. Это улучшенный вариант запроса GETNEXT.

SET — с помощью этого запроса менеджер изменяет или присваивает устройству новые данные.

RESPONSE — сообщение от агента, высылаемое в ответ на запрос данных.

TRAP — уведомление о произошедшем событии или ошибке. Агент отправляет его сразу после наступления события, не дожидаясь запроса менеджера. Менеджер никак не подтверждает получение сообщения, что может стать проблемой.

INFORM — сообщение, аналогичное TRAP, но с подтверждением получения. Агент будет отправлять уведомление, пока менеджер не подтвердит, что оно дошло.

INFORM, GETBULK — есть только во второй и третьей версиях протокола SNMP.

Система мониторинга Zabbix. Практическая работа.


<http://192.168.15.190/zabbix>


Логин: user<XY>


Пароль: academyNAG2023







 **ЕКАТЕРИНБУРГ**
ул. Краснолесья, 12а
(ТЦ Краснолесье), 4-й этаж
+7 (343) 379-98-38
sales@nag.ru

 **МОСКВА**
Семёновская площадь, 1а
БЦ «Соколиная Гора», 13 этаж
+7 (495) 950-57-11
msk@nag.ru

 **САНКТ-ПЕТЕРБУРГ**
Большой Сампсониевский
просп., 28/2, офис 325
+7 (812) 918-98-38, +7 (812) 406-8-100
spb@nag.ru

 **РОСТОВ-НА-ДОНУ**
ул. Береговая, 8, офис 409
+7 (863) 270-45-21
rostov@nag.ru

 **НОВОСИБИРСК**
ул. Гоголя, 51
+7 (383) 251-02-56
ns@nag.ru

 **КАЗАХСТАН, АЛМАТЫ**
ул. Кунаева, 32, офис 217
+7 727 344-34-44
sales@nag.kz

 **УЗБЕКИСТАН, ТАШКЕНТ**
Миришкор 2-й тупик, 17/19
+998 91-004-70-08
sales@nag.uz