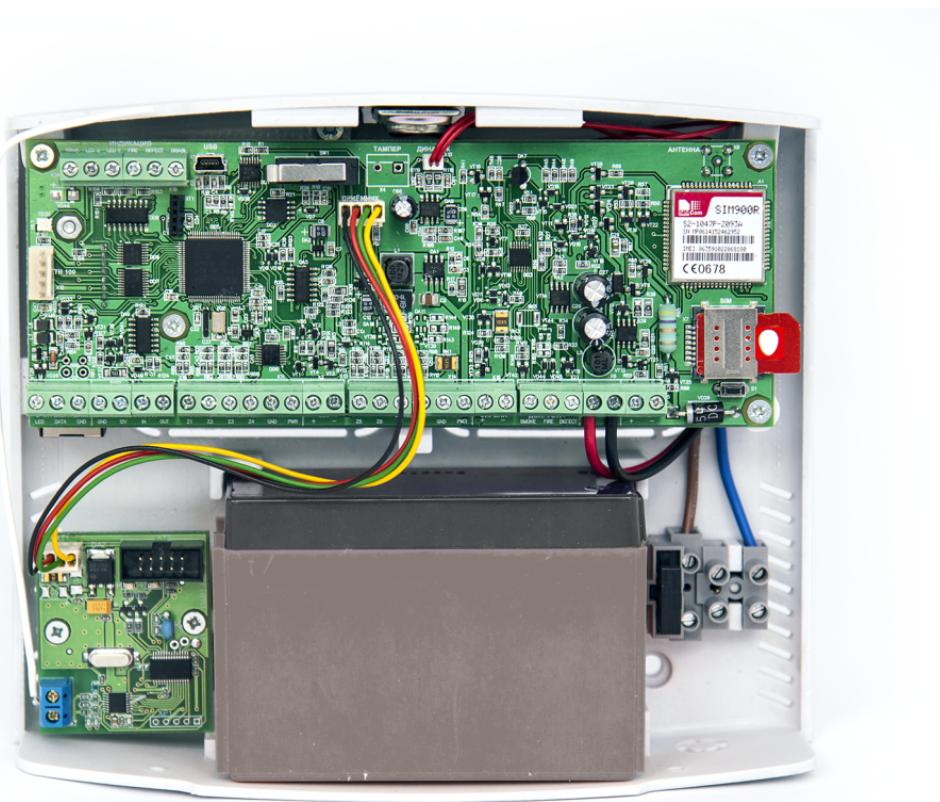


Nord GSM / Nord GSM WRL

OPERATION MANUAL



C.Nord

4 июля 2019 г.

Содержание

1 Descripción técnica	5
1.1 Uso y posibilidades	5
1.2 Alimentación eléctrica	5
1.3 Canales de transmisión de avisos	6
1.4 Posibilidades técnicas	6
1.5 Características técnicas principales	7
1.5.1 Kit de suministro	8
1.5.2 Etiquetaje	9
1.5.3 Embalaje	9
2 Control del equipo	10
2.1 Llave TM	10
2.1.1 Indicación de lectura	10
2.1.2 Indicación de errores	10
2.1.3 Indicación de desarme	11
2.1.4 Indicación de arme	11
2.1.5 Indicación de modo de guardia	11
2.1.6 Recepción del estado del objeto	13
2.1.7 Recepción del estado de la partición	13
2.1.8 Arme y desarme	13
2.1.9 Indicación acústica y por voz	14
2.1.10 Botón de emergencia	15
2.2 Клавиатура K16-LCD	16
2.2.1 Взятие и снятие	16
2.2.2 Светодиодная индикация	17
2.2.3 Звуковая индикация	18
2.2.4 Экранная индикация	18
2.3 Teclado inalámbrico CN-K	21
2.3.1 Arme y desarme	22
2.3.2 Recepción del estado	23
2.3.3 Botón de emergencia	24
2.3.4 Desactivación de la iluminación y el sonido	24
2.4 Llavero inalámbrico	24
2.5 Aplicación móvil MyAlarm	24

3 Montaje y primera puesta en marcha	26
3.1 Esquema de montaje del equipo	26
3.2 Conexión de zonas por cable	27
3.2.1 Zona normal cerrada y normal abierta	27
3.2.2 Resistencias terminales	27
3.2.3 Zona sin resistencias terminales	28
3.2.4 Zona con una resistencia terminal	28
3.2.5 Zona con dos resistencias terminales	29
3.2.6 Zonas por cable en el configurador	29
3.3 Conexión de avisadores de incendio	30
3.3.1 Avisadores de incendio de cuatro cables	30
3.3.2 Avisadores de incendio de dos cables	30
3.4 Conexión de sensores de temperatura	31
3.5 Conexión del expansor “EW-12”	31
3.6 Conexión del expansor “EW-8”	35
3.7 Configuración del canal GSM	36
3.7.1 Instalación de tarjetas SIM	36
3.7.2 Verificación del nivel de la señal GSM	37
3.7.3 Conexión de la antena GSM remota	37
3.8 Conexión del lector Touch Memory	38
3.9 Conexión de teclados por cable	38
4 Actualización del software	39
4.1 Conexión del equipo a la computadora	39
4.2 Instalación del controlador en Windows XP y Windows 7	39
4.3 Instalación del controlador en Windows 8	44
4.4 Utilidad de actualización del software	47
5 Configuración del dispositivo	49
5.1 Panel de control y panel de pestañas	49
5.1.1 Panel de control	49
5.1.2 Panel de pestañas	51
5.2 Zonas	52
5.2.1 Expansores	52
5.2.2 Numeración de zonas	52
5.2.3 Activación y desactivación de la zona	53
5.2.4 Tipo de zona	53
5.2.5 Estado normal de la zona	55
5.2.6 Resistencias terminales	55

5.2.7	Retraso de entrada	56
5.2.8	Retraso de salida	56
5.3	Dispositivos inalámbricos	58
5.3.1	Conexión del dispositivo al equipo	58
5.3.2	Retransmisor	59
5.3.3	Recomendaciones de montaje	59
5.4	Usuarios	60
5.5	Particiones	62
5.5.1	Control de particiones	62
5.6	Varios	63
5.6.1	Intervalos	63
5.6.2	Alimentación de reserva	66
5.6.3	Control e indicación	69
5.6.4	Protección de la configuración	69
5.7	Security Center	72
5.7.1	Identificación del equipo	72
5.7.2	Parámetros de transmisión por GPRS	73
5.7.3	Parámetros de transmisión por Ethernet	74
5.7.4	Parámetros de transmisión en el canal CSD GSM	75
5.7.5	Parámetros de transmisión en el canal de voz GSM	75
5.7.6	Parámetros de transmisión por SMS	76
5.7.7	Cambio de canales de comunicación	76
5.8	Radio	78
5.8.1	Configuración del canal de radio	78
5.8.2	Números de particiones de los objetos	79
5.8.3	Equipo en cuerpo metálico	79
5.9	Nube	80
5.10	Ethernet	81
5.11	Operadores GSM	82
5.12	Sistema automático	83
5.12.1	Notificador	83
5.12.2	Sirena	85
5.12.3	Varios	85
5.13	История событий	88
5.14	Панель состояния	89
5.14.1	Каналы связи	89
5.14.2	Проводные шлейфы	89
5.14.3	Беспроводные устройства	90

6 Удалённый доступ к прибору	91
6.1 Описание технологии удалённого доступа	91
6.1.1 Канал связи прибор ↔ пульт	91
6.1.2 Канал связи прибор ↔ «Облако»	92
6.1.3 Канал связи пульт ↔ «Облако»	92
6.2 Настройка удалённого доступа	92
6.2.1 Создание инженера	92
6.2.2 Выдача разрешений инженеру	94
6.3 Удалённое конфигурирование устройств	94
6.3.1 Выбор объекта для конфигурирования	94
6.3.2 Работа с конфигурацией	95
6.3.3 Особенности работы	96
6.4 Удалённое обновление ПО на устройстве	96
6.4.1 Информация об объектах на пульте	96
6.4.2 Процесс удалённого обновления ПО на устройстве	97
6.4.3 Обновление ПО на выбранном объекте	97
6.4.4 Обновление ПО на всех объектах	98
6.4.5 Остановка процесса обновления	99
7 Коды событий	100

1 Descripción técnica

1.1 Uso y posibilidades

El equipo “Nord GSM” está destinado para usarse en calidad de dispositivo principal del complejo de seguridad - contra incendios - equipo de recepción - control de seguridad - contra incendios, que se instala en locales en objetos protegidos.

Al equipo se pueden conectar diferentes avisadores y dispositivos de seguridad, contra incendios y tecnológicos por cable e inalámbricos. Para la conexión de dispositivos inalámbricos se usa el expansor por radio opcional “CN-Radio”.

El equipo puede crear y transmitir a la consola de seguridad mensajes sobre eventos que se producen durante el proceso de su explotación y relacionados con:

- arme del dispositivo o desarme del equipo;
- cambio del estado de sus zonas de seguridad
- cambio del estado de sus fuentes de alimentación eléctrica (principal y de reserva);
- problemas en el funcionamiento de los canales de comunicación usados por el producto y aparición de otros tipos de fallos;
- activación y recuperación del estado del sensor de la apertura de su cuerpo.

El equipo de seguridad realiza la transmisión de notificaciones a la consola de seguridad mediante un comunicador GSM/GPRS integrado a través de un canal de voz, SMS o GPRS. Existe la posibilidad de transmitir mensajes a través de la red Ethernet mediante el módulo “Adaptador Ethernet” opcionalmente instalable en el producto, así como a través del canal de radio mediante un transmisor de radio instalable en el producto con diapasón SV, VHF o UHF.

El equipo dispone de una fuente de alimentación ininterrumpida y realiza el servicio automático de la fuente de alimentación interrumpida instalada en su cuerpo durante todo el plazo de su explotación. El producto es capaz de proporcionar la alimentación eléctrica de los módulos de comunicación conectables (comunicadores) y los dispositivos de expansión de sus posibilidades funcionales en los marcos de las potencias consumidas admitidas.

1.2 Alimentación eléctrica

La principal fuente de alimentación eléctrica del producto es la red monofásica de corriente alterna de 220 V 50 Hz con una gran tensión de (127÷264) V.

En calidad de fuente de alimentación eléctrica de reserva pueden usarse:

- batería hermética de plomo y ácido que cumple con el estándar IEC 1056-1, tensión nominal ($12,6 \pm 0,6$) V. La batería se instala en el cuerpo del producto;
- fuente de alimentación ininterrumpida externa (UPS) con tensión nominal de salida de 12 V y carga de corriente permisible no inferior a 1,5 A con una batería del correspondiente sistema químico instalada en la misma, teniendo en cuenta que la UPS externa debe conectarse al producto en vez de la batería.

Diapasón de tensiones admitidas de la fuente de reserva al poner en marcha el producto en caso de que no esté presente la fuente principal - de 10,0 V a 14,4 V.

La capacidad recomendada de la batería, ubicada en el cuerpo de plástico del producto - 1,2 o 2,2 (A*h), por ejemplo DELTA DTM 12022.

El producto proporciona un servicio automático de la batería que se instala en el mismo, que incluye:

- etapa de carga “suave” de una batería profundamente descargada con una corriente de (100 ± 20) mA hasta alcanzar en ésta una tensión de ($11,5 \pm 0,2$) V;
- consiguiente carga de la batería en la segunda etapa con una corriente de (230 ± 25) mA;

5 • alcance de la tensión final en la batería al final del ciclo de su carga de ($14,0 \pm 0,2$) V con su consiguiente mantenimiento en el diapasón de ($13,6 \div 14,0$) V con el fin de compensar la corriente de su autodescarga;

- posibilidad de desconexión automática de la batería descargada en el caso de que no esté presente la fuente principal de alimentación eléctrica al llegar la tensión en ésta a ($9,0 \pm 0,3$) V;
- limitación de la corriente consumida por el producto de la desconexión automática de la batería, con un valor que no supera el valor “suave” por 25 mkA;

- resistencia de ruptura y cortocircuitos en el circuito de la batería durante un tiempo ilimitado, con ello la alimentación del producto se realizará a través de la fuente principal; • protección contra la “polaridad inversa” en caso de una conexión errónea a los bornes de la batería o la UPS externa; • tests automáticos periódicos de la batería y evaluación de su estado por conjunto de varios parámetros con el consiguiente envío de las correspondientes notificaciones al programa de la consola. La opción puede ser desconectada al realizar la configuración del producto;
- “entrenamiento” automático de la batería mediante la toma periódica a corto plazo del impulso de la corriente durante la carga de baja resistencia integrada en el producto. Este procedimiento realiza el algoritmo de carga por corriente asimétrica alterna, favorable para la plenitud de la carga y para la duración del ciclo vital de la batería operada en modo buffer. La opción puede ser desconectada al realizar la configuración del producto.

Si en calidad de fuente de reserva de alimentación eléctrica se usa una UPS externa, el producto sigue controlando periódicamente el hecho de su conexión, pero no realiza:

- la carga de la fuente externa; • su test periódico con la verificación del nivel actual de carga y el valor de la resistencia interna.

1.3 Canales de transmisión de avisos

El envío de avisos por el producto puede realizarse a través de los siguientes canales independientes de comunicación:

- a través de redes de comunicación de telefonía móvil de estándar GSM 900/1800 de dos diferentes operadores mediante el modem GSM integrado;
- a través de la red Ethernet mediante el módulo “Adaptador Ethernet” opcionalmente instalable en el producto, que se conecta a una línea especial de conectores de la placa principal del producto;
- a través del canal de radio en los diapasones SV, VHF, UHF mediante un transmisor de radio que se instala adicionalmente, conectado al conector de la interfaz “TR-100 OUT” del producto (para el producto en cuerpo metálico).

El producto en cuerpo de plástico va equipado con una pequeña antena GSM de látigo sin alimentador con conector de ángulo recto tipo SMA-male, conectada al conector tipo SMA-female. Para los productos en cuerpo de plástico se prevé la posibilidad de conexión de una antena remota de tipo dipolo (con conector del mismo tipo) con el fin de mejorar la calidad de comunicación con la estación base del operador de telefonía celular. El producto en cuerpo metálico va equipado exclusivamente con una antena remota de tipo dipolo.

Para la transmisión de eventos a la consola de monitoreo el equipo puede usar los siguientes canales de comunicación:

- GPRS;
- CSD (para equipos versión hardware 5.1, 5.2, 5.7);
- VOICE (canal de voz con uso de codificación DTMF);
- SMS.

En modo de transmisión de notificaciones por paquetes (GPRS) se realiza el cifrado del contenido.

El equipo dispone de un sujetador de tarjetas SIM de dos niveles, en el cual se pueden instalar dos tarjetas SIM de diferentes operadores de comunicación móvil. La elección de la tarjeta SIM activa se realiza de forma automática, de conformidad con el algoritmo establecido de funcionamiento del módulo de comunicación móvil. Aparte de esto está previsto un cambio incondicional a otra tarjeta SIM al pulsar el usuario el botón ubicado junto al sujetador de tarjetas SIM.

El equipo puede valorar el nivel de la señal en las redes de comunicación móvil de los operadores que se usan en el lugar de la instalación del dispositivo de una forma separada para cada una de las dos tarjetas SIM y mostrar la valoración obtenida en la interfaz del configurador.

1.4 Posibilidades técnicas

- configuración de hasta 16 zonas de alarma por cable que sirven para la recepción de avisos que provienen de avisadores analógicos manuales y automáticos de seguridad y contra incendios, equipos de recepción - control de seguridad y de seguridad - contra incendios a través de las salidas del relé de la Consola de monitorización centralizada;
- conexión de hasta 31 dispositivo inalámbrico;
- configuración de hasta 32 particiones con la posibilidad de su arme y desarme independiente;
- control de dispositivos de ejecución y medios del sistema automático mediante las salidas de control de tipo “colector abierto”;
- control del modo de funcionamiento del producto mediante los teclados por cable K16-LCD, K14-LED, teclado inalámbrico CN-K, llaves electrónicas Touch

Memory, lector de tarjetas proximity, así como llaveros inalámbricos; • alarma acústica y óptica en modo “Alarma” e “Incendio”; • control de apertura del cuerpo del producto; • control del correcto funcionamiento de las zonas de alarma con detección automática de ruptura o cortocircuito, señalización óptica y acústica de fallo, creación de avisos para la consola de seguridad sobre el fallo; • aviso acústico y óptico al armar el sistema de seguridad del producto y desarmar el sistema de seguridad del producto; • almacenamiento de la información en el registro de eventos.

1.5 Características técnicas principales

- Cantidad mínima de las zonas de seguridad por cable que sirve el producto, previstas para la conexión de diferentes avisadores - 8;
- Cantidad de zonas de seguridad que sirve el producto, en caso de ser equipado con expansor de cantidad de zonas por cable - 16;
- Resistencia total máxima permitida de dos cables de cada zona - no más de 330 Ohm;
- Cantidad de dispositivos terminales inalámbricos (autónomos), soportados por el producto al instalar en éste un bloque de canal de radio de expansión de zonas de alarma “CN-Radio” - hasta 31;
- Para un trabajo conjunto con el producto en la versión “Nord GSM/WRL” (con el expansor de radio “CN-Radio” instalado) pueden usarse los siguientes dispositivos terminales de canal de radio;

- avisador de seguridad manual "CN-KeyFob";
- avisador de seguridad óptico electrónico de volumen "CN-PIR";
- avisador de seguridad óptico electrónico de volumen de calle "CN-PIR-Outdoor";
- avisador de seguridad de contacto magnético "CN-Magnetic";
- avisador de seguridad acústico superficial "CN-Glass";
- avisador de incendio "CN-Smoke";
- avisador de incendio manual "CN-Fire";
- avisador de inundación "CN-Flood";
- avisador de temperatura "CN-Celsius";
- retransmisor de avisos "CN-Repeater";
- sirena "CN-Siren";
- teclado "CN-Keypad".

> El expansor de radio opcional "CN-RADIO" se conecta a la placa principal del producto mediante un conector

- Cantidad de estados de zonas por cable controladas por el producto - hasta cuatro (“norma”, “alarma”, “ruptura”, “corte”). Con ello el tipo de cada una de las zonas organizadas - cerrada normal o abierta normal, así como la cantidad de resistencias terminales, con una o dos resistencias terminales - se establece por el usuario al realizar la configuración del producto; • El producto permite la conexión en zonas de seguridad por cable de sensores contra incendio de cuatro cables, proporcionando la posibilidad de su reinicio automático (reseteo del estado de alarma) de la commutación en las líneas de su alimentación eléctrica. • La corriente máxima de consumo por todos los sensores por cable que se conectan al producto se limita por el valor nominal del fusible térmico autorecuperable y no debe superar los 200 mA; • El producto dispone de un microinterruptor instalado en su placa, que desempeña el papel de sensor de apertura del cuerpo (tamper).

> Adicionalmente se prevé la posibilidad de instalar en la placa del producto un bloque de terminales para

- El producto dispone de memoria no volátil para el almacenamiento de los avisos que se crean en el mismo; • El producto proporciona el soporte del protocolo 1 Wire en el rango “master” en el conector de la correspondiente interfaz, permitiendo realizar su arme y desarme, por ejemplo por dispositivos de la serie DS1990 A, conectar sensores remotos de temperatura, dispositivos de expansión hardware de puertos del controlador, etc., (el soporte de unos u otros dispositivos en el bus 1-Wire se determina por la versión software del controlador del producto).

La línea “LED” de la interfaz, 1-Wire está protegida del cortocircuito y sirve para la conexión de un LED externo, que refleja la condición del estado del producto, con una corriente de consumo de hasta 8 mA (por ejemplo, LED situado en la apertura del lector TM); • El producto dispone de bornes para la conexión de teclados por cable K16-LCD y K14-LED. Las líneas de fuerza de la interfaz del teclado están protegidas contra el cortocircuito por un fusible térmico autorecuperable, la ausencia o la alteración del tráfico en la interfaz del teclado se detecta por el controlador del producto; • Al producto se puede conectar una sirena piezoelectrónica para la confirmación acústica del estado “Alarma” con una corriente de consumo de hasta 200 mA con ello, por el producto se detectan tales fallos en el circuito de su conexión, como roturas y cortos circuitos, tanto si está presente o no está presente la señal “Alarma”. La salida para la conexión de la sirena está protegida por un fusible térmico autorecuperable; • El producto tiene siete salidas discretas controlables de tipo “colector abierto”, que permiten conectar al producto una carga conmutada, por ejemplo, relés electromagnéticos, equipos acústicos u óptico - electrónicos. Corriente entrante máxima permitida de carga de salidas discretas - 500 mA; tensión continua máxima permitida conectada a las salidas - mas 50 V; • En la placa principal está instalado un LED tecnológico multifuncional de tres colores, que sirve para reflejar el estado actual del producto y los valores de verificación de algunos parámetros controlables por el mismo; • El producto proporciona un soporte por voz al usuario (personal de servicio) mediante la reproducción a través del cabezal dinámico integrado de archivos de audio en caso de detectar problemas que interfieren en la explotación normal del producto, por ejemplo, al detectar fallos en las zonas de seguridad concretizando su carácter y el lugar de detección, al llegar a un saldo negativo en la cuenta por los servicios de seguridad, etc. • El producto dispone de un conector vertical de tipo “mini USB B” para la posibilidad de su configuración después de la conexión al puerto USB de la computadora; • Mediante el software especializado es posible realizar la modificación remota de los parámetros de configuración del producto, así como la actualización del software de su controlador; • El producto está diseñado para funcionar en un modo de trabajo ininterrumpido (24 horas) en el diapasón de temperaturas funcionales (sin tener en cuenta las limitaciones de temperaturas para la fuente de alimentación eléctrica de reserva) desde 30 °C bajo cero hasta 50 °C sobre cero;

> El diapasón permitido de temperaturas de explotación del producto con la fuente de alimentación de reserva

- Tamaños dimensionales del cuerpo del producto de plástico, mm, no más de - 188x200x62; • Masa del producto en cuerpo de plástico (sin fuente de alimentación eléctrica de reserva, cable de alimentación y envase), kg, no más de 0,6; ## Kit de suministro, etiquetaje y envase

1.5.1 Kit de suministro

Dispositivo de recepción - control de seguridad - contra in	cendios «Nord GSM» / «Nord GSM WRL» 1 un.
Resistor 0,25 W (0,16 W) – 2,2 kOhm	16 un.
Resistor 0,25 W (0,16 W) – 4,3 kOhm	16 un.
Inserción fusible VPB 6-7, 1 A, 250 V	1 un.
Fijador de plástico de la batería con una capacidad de 1,2	Ah en el cuerpo del producto 1 un.
Kit de toma de tierra ZK-15(m)	1 un.
Kit de elementos de fijación (m)	1 un.
Antena remota GSM 2J520-SMA-male (o similar) (m)	1 un.
Ficha técnica	1 un.
Embalaje	1 un.

Observaciones: (m) - para productos en cuerpo metálico

1.5.2 Etiquetaje

La placa de circuito impreso del producto dispone de una marca de polaridad de salidas de los bloques de terminales y su destinación.

El producto tiene una marca en forma de etiquetas con el nombre del producto y un código de barras. Las etiquetas están pegadas en la parte frontal de la placa de circuito impreso del producto y en el cuerpo. Aparte de esto, la etiqueta está pegada en la ficha técnica del producto.

1.5.3 Embalaje

El producto se suministra en una caja de cartón individual. Antes de ser ubicado en la caja, el producto en cuerpo de plástico se envasa en una bolsa de polietileno con burbujas de aire, que proporciona una protección adicional al producto contra daños y alta humedad durante el almacenamiento y el transporte. En la caja junto con el producto se ponen los accesorios de conformidad con el kit de suministro.

2 Control del equipo

Para armar / desarmar el sistema de alarma del equipo se pueden usar los siguientes dispositivos de control:

- llave TM;
- teclado K14-LED;
- teclado K16-LCD;
- llavero inalámbrico;
- dispositivo móvil MyAlarm.

2.1 Llave TM



Puc. 1: Dibujo 1: Lector - TM y llave - TM

El equipo dispone de una interfaz integrada para la conexión de lectores de llaves TM. Aparte de esto, en el dispositivo se prevé la posibilidad de conectar un indicador LED que se ubica directamente en el cuerpo de algunas marcas de lectores de llaves TM.

El indicador LED ubicado en el cuerpo del lector TM, sirve para la indicación de la lectura de la llave TM, el arme y desarme del sistema de seguridad, así como para la indicación del estado actual del equipo.

Mediante una llave TM se puede armar el sistema de seguridad o desarmar el sistema de seguridad de una partición. Si un usuario necesita tener la posibilidad de armar o desarmar varias particiones al mismo tiempo, hay que configurar las correspondientes reglas en el apartado “Sistema automático”.

2.1.1 Indicación de lectura

Si la operación de lectura de la llave finaliza con éxito, el equipo lo indica, independientemente de si la llave fue encontrada en la memoria del equipo o no. En otras palabras, en caso de que se produzca una lectura con éxito el equipo simplemente confirma que al lector fue acercada una llave y esta llave fue leída.

Indicación de una lectura con éxito de la llave TM: LED “parpadeante” (se enciende por 0,1 seg, permanece encendido, después se apaga por 0,1 seg) durante 1 segundo.

2.1.2 Indicación de errores

Al realizar la lectura de la llave, pueden producirse los siguientes errores:

- llave no encontrada en la memoria del equipo; • denegación de arme.

Indicación de error: LED “parpadeante” (se enciende por 0,5 seg, después se apaga por 0,5 seg) durante 3 segundos.

2.1.3 Indicación de desarme

Si ha sido leída la llave, mediante la cual se puede cambiar el estado de la partición y está armado el sistema de seguridad de esa partición, se desarma el sistema de seguridad de la partición.

La indicación de desarme se realiza después de que se haya realizado la indicación de lectura.

Indicación de desarme: el LED se enciende por 5 segundos y se apaga.

Después de que se realice la indicación de desarme del sistema de seguridad, se enciende la indicación del modo de guardia.

2.1.4 Indicación de arme

Si se lee la llave con la cual se puede cambiar el estado de la partición, en caso de que en la partición no haya zonas con retraso de salida, se realiza el arme del sistema de seguridad de la partición. Si en la partición hay zonas con retraso de salida, empieza la cuenta del intervalo de retraso; el arme del sistema de seguridad se realiza al finalizar el retraso de salida.

La indicación de arme del sistema de seguridad depende de la cantidad de particiones configuradas en el equipo.

Una partición

Si en el equipo sólo está configurada una partición, después de su arme el LED se enciende y permanece encendido constantemente: se enciende la indicación del modo de guardia con la única partición armada.

Varias particiones

Si en el equipo están configuradas varias particiones, la indicación después del arme del sistema de seguridad de la partición actual depende de si quedan particiones desarmadas o no.

Si todas las particiones están armadas, el LED se enciende y permanece encendido de forma continua: se apaga la indicación del modo de guardia con varias particiones, todas las particiones están armadas.

Si existe aunque sea una partición que no está armada, el LED se enciende y permanece encendido durante 20 segundos. A continuación se enciende la indicación del modo de guardia con varias particiones, parte de las cuales está desarmada.

Denegación del arme

La “denegación del arme” - es la imposibilidad de armar el sistema de seguridad del objeto, si la alarma de seguridad en el objeto no funciona correctamente, o si el arme del sistema de seguridad está prohibido por el impago de los servicios de seguridad.

Están previstos los siguientes motivos de denegación del arme:

- fallo de una o varias zonas;
- alarma en una o varias zonas;
- ausencia de comunicación con el programa de la consola por el canal IP;
- ausencia de 220 V en el objeto;
- impago de los servicios de seguridad;
- está abierto el cuerpo del equipo.

2.1.5 Indicación de modo de guardia

Durante el tiempo de la indicación de lectura, error de arme/desarme, arme y desarme, la indicación del modo de guardia se interrumpe.

La indicación del modo de guardia depende de la cantidad de particiones configuradas en el equipo.

Una partición

Si en el equipo sólo está configurada una partición, el LED indica el estado de la partición, la existencia de alarma durante el período de seguridad y el fallo de las zonas;

- LED encendido de forma ininterrumpida, si la partición está armada;
- LED apagado, si la partición está desarmada;
- LED “parpadeante” [“blink”], si hay fallos en las zonas;
- LED “parpadeante”, si después de armar la partición se produjo una alarma y el sistema de seguridad de la partición no fue desarmado

“Parpadea” significa que el LED se enciende por 1 segundo, después de lo cual se apaga por 1 segundo, después de lo cual, de nuevo se enciende por 1 segundo, etc.

Varias particiones

Si en el equipo están configuradas varias particiones, se indica sólo el estado del arme de todo el dispositivo, presencia de alarma, cuando todo el equipo estaba armado, así como los fallos de las zonas.

- LED encendido de forma ininterrumpida, si todas las particiones del equipo están armadas;
- LED apagado, si aunque sea una partición está desarmada;
- LED “parpadeante”, si hay fallos en las zonas;
- LED “parpadeante”, si después de armar el sistema de seguridad de todo el equipo se produjo una alarma y la partición donde se produjo la alarma no fue desarmada.



Puc. 2: Dibujo 2: Teclado K14-LED

Mediante el teclado K14-LED el usuario puede realizar las siguientes tareas:

- conocer el estado de la partición (armada / desarmada);
- armar la partición o desarmar la partición;
- informarse de un retraso de entrada o salida que acaba de empezar o continua;
- conocer el estado de seguridad de todo el equipo;

En el teclado K14-LED se ubica un LED verde y otro rojo:

- El LED rojo permanece encendido constantemente si todas las particiones del equipo están armadas.
- Al desarmar la partición se apaga el LED rojo y se enciende el verde.
- Los LEDs rojo y verde parpadean al mismo tiempo si se produjo un error. Por ejemplo, al introducir un código incorrecto del usuario o en caso de denegación del arme del sistema de seguridad.

2.1.6 Recepción del estado del objeto

Para recibir la información sobre el estado del objeto hay que pulsar el botón **i**:

- si en el equipo están configuradas las particiones y todas las particiones están armadas, el teclado reproducirá: “Sistema de seguridad del objeto armado” y encenderá el LED rojo.
- si en el equipo están configuradas las particiones y todas las particiones están desarmadas, el teclado reproducirá: “Sistema de seguridad del objeto desarmado” y encenderá el LED verde.
- si en el equipo están configuradas las particiones y algunas de ellas están armadas, y otras desarmadas, el teclado muestra la indicación de error.
- si en el equipo no están configuradas las particiones, el teclado muestra la indicación de error.

2.1.7 Recepción del estado de la partición

Para recibir la información sobre el estado de la partición hay que pulsar el botón del número de la partición y el botón **i**:

- si la partición existe, el teclado reproduce su estado y enciende el correspondientes LED.
- si la partición no existe, el teclado muestra la indicación de error.

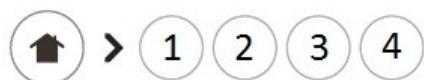
2.1.8 Arme y desarme

En el equipo está realizada la posibilidad de arme y desarme del sistema de seguridad de varias particiones con un código de usuario. El ajuste de particiones que pueden ser armadas o desarmadas con un código en concreto, se realiza al realizar la configuración del equipo.

Arme del sistema de seguridad

Para armar la partición hay que pulsar “casita” e introducir el código del usuario.

- si el código es correcto, el sistema de seguridad del objeto (partición) será armado, el teclado confirmará el arme mediante la activación del LED rojo. O se activará la cuenta del intervalo de retraso de salida, que va acompañada por una indicación acústica y LED.
- si el código es incorrecto o al usuario al que le pertenece ese código, le corresponde más de una partición, el teclado mostrará un error.
- si el arme del sistema de seguridad no es posible, el teclado mostrará un error.



Puc. 3

Si al código de usuario están asignadas varias particiones, primero el usuario debe pulsar el botón “casita”, elegir el apartado, cuyo estado desea cambiar y a continuación teclear el código.



Puc. 4: Пример взятия с выбором раздел

Denegación del arme del sistema de seguridad

La “Denegación del arme” - es la imposibilidad de armar el sistema de seguridad del objeto, si la alarma de seguridad en el objeto no funciona correctamente, o si el arme del sistema de seguridad está prohibido por el impago de los servicios de seguridad.

Están previstos los siguientes motivos de denegación del arme:

- fallo de una o varias zonas;
- alarma en una o varias zonas;
- ausencia de comunicación con el programa de la consola por el canal IP;
- ausencia de 220 V en el objeto;
- impago de los servicios de seguridad;
- está abierto el cuerpo del equipo.

Desarme del sistema de seguridad

Si el usuario puede controlar sólo una partición, para desarmar el sistema de seguridad hay que introducir el código del usuario.

- si el código es correcto, el sistema de seguridad del objeto (partición) será desarmado. El teclado confirmará el desarme mediante la activación del LED verde.
- si el código es incorrecto o el usuario al que le pertenece ese código, puede controlar varias particiones, el teclado mostrará un error.



Puc. 5

Si el usuario puede controlar varias particiones, para desarmar el sistema de seguridad hay que teclear el número de la partición y a continuación # e introducir el código del usuario.

- Si el código es correcto, el sistema de seguridad de la partición será desarmado. El teclado confirmará el desarme mediante la activación del LED verde.
- Si se vuelve a desarmar el sistema de seguridad de la misma partición, el teclado mostrará su estado: se encenderá el LED verde.



Puc. 6: Ejemplo de desarme con selección de partición

La cuenta del intervalo de retraso de entrada o intervalo de retraso de salida se indica mediante un sonido intermitente que se reproduce durante todo el intervalo de retraso. La indicación acústica de retraso de entrada o salida se desconecta al pulsar cualquier botón del teclado.

2.1.9 Indicación acústica y por voz

El teclado dispone de un altavoz integrado, a través del cual se realiza la indicación por voz e indicación por el zumbador. La pulsación de teclas en el teclado va acompañada con una señal acústica que confirma la pulsación.

Con voz se indica:

- Arme del sistema de seguridad y desarme del sistema de seguridad de particiones y el objeto en general;

- Denegación de arme del sistema de seguridad;
- Advertencias sobre saldo insuficiente al armar el sistema de seguridad;
- Estado de la partición o del objeto en general (al pulsar las tecla i).

En el teclado se está prevista la función de ajuste del volumen del altavoz integrado. Ajuste de cinco niveles - empezando por el estado “desactivado” hasta los niveles de volumen del primero hasta el cuarto. La selección del nivel de sonido se realiza mediante la combinación de las teclas “#” y “9”.

2.1.10 Botón de emergencia

Si en la configuración del equipo está permitido el uso del teclado en calidad de botón de emergencia, para la activación hay que pulsar y mantener pulsados durante 3 segundos los botones de las “casitas”, la activación de los LEDs verde y rojo durante 1 segundo acompañada con sonido confirma que fue pulsando el botón de emergencia.

Si en la configuración del equipo está prohibido el uso del teclado en calidad de botón de emergencia, el teclado mostrará un error.

2.2 Клавиатура K16-LCD



Рис. 7: Клавиатура K16-LCD

С помощью клавиатуры K16-LCD пользователь может выполнить следующие задачи:

- узнать состояние раздела (взят / снят);
- взять раздел под охрану или снять раздел с охраны;
- узнать о начавшейся или продолжающейся задержке на вход или выход;
- узнать состояние всего прибора;
- узнать о наличии неисправности электропитания прибора;
- узнать о наличии неисправностей.

2.2.1 Взятие и снятие

В приборе реализована возможность взятия и снятия с охраны нескольких разделов одним кодом пользователя. Настройка разделов, которые могут быть взяты или сняты с охраны конкретным кодом, выполняется при конфигурировании прибора.

Взятие и снятие без выбора раздела

Если за кодом пользователя закреплен только один раздел, то при наборе кода будет выполнена попытка изменить состояние охраны этого раздела:

- если раздел взят под охрану, то при наборе кода он будет снят с охраны;
- если раздел снят с охраны, то при наборе кода начнется процедура взятия раздела под охрану.

Если взятие под охрану разрешено, то выполняется взятие под охрану, либо включается отсчет интервала задержки на выход, которая сопровождается звуковой, светодиодной и экранной индикацией.

Если взятие под охрану запрещено, то выполняется звуковая индикация отказа от взятия, а на экране клавиатуры отображается причина, по которой взятие невозможна.

Взятие и снятие с выбором раздела

Если за кодом пользователя закреплено несколько разделов, то сначала пользователь должен выбрать раздел, состояние которого он хочет изменить, а после этого набрать код.

Для выбора раздела пользователь должен сначала ввести номер раздела, состояние которого он хочет изменить, а после этого нажать на кнопку «#».

Предположим, что пользователь хочет снять с охраны раздел номер 2 с помощью кода 1234.

Для этого ему нужно нажать на клавиатуре следующую последовательность кнопок: 2#1234

Если пользователь набрал правильный код, за которым закреплено несколько разделов, но предварительно не выбрал раздел, состояние которого он хочет изменить, то такой код обрабатывается, как неправильный.

Отказ от взятия

«Отказ от взятия» – это невозможность взять объект под охрану, если охранная сигнализация на объекте неисправна, либо взятие под охрану запрещено из-за отсутствия оплаты за услуги охраны.

Предусмотрены следующие причины отказа от взятия:

- неисправность одного или нескольких шлейфов;
- тревога в одном или нескольких шлейфах;
- отсутствие связи с пультовой программой по IP-каналу;
- отсутствие 220В на объекте;
- отсутствие оплаты за услуги охраны;
- открыт корпус прибора.

2.2.2 Светодиодная индикация

На клавиатуре K16-LCD расположены два светодиода: «Авария» и «Охрана».

Светодиод «Охрана»

Для светодиода предусмотрено два режима индикации: дежурный режим и режим взятия.

В дежурном режиме светодиод «Охрана» отображает состояние охраны всего прибора:

- если для прибора сконфигурирован только один раздел, то светодиод включен, если этот раздел взят под охрану, и выключен, если снят;
- если для прибора сконфигурировано несколько разделов, то светодиод включен, если все разделы взяты под охрану, и выключен, если хотя бы один раздел снят с охраны;
- если ни одно из условий, описанных выше, не выполняется, то светодиод выключен.

В режиме взятия светодиод «быстро мигает» в течение интервала задержки на выход.

Светодиод «Авария»

Светодиод предназначен для индикации отсутствия основного питания, а также для индикации неисправности резервного источника питания:

- светодиод включен, если присутствует основное питание, а источник резервного питания отсутствует, разряжен или неисправен;
- светодиод «медленно мигает», если отсутствует основное питание;

- светодиод выключен, если присутствует основное питание, а неисправности резервного питания отсутствуют.

Неисправность источника резервного питания индицируется только в том случае, если в настройках прибора в качестве источника резервного питания указана аккумуляторная батарея, а также включен контроль качества резервного источника питания.

2.2.3 Звуковая индикация

Нажатие кнопок на клавиатуре сопровождается звуковым сигналом, подтверждающим нажатие.

Отсчет интервала задержки на вход или интервала задержки на выход индицируется прерывистым звуком, который воспроизводится в течение всего интервала задержки. Звуковая индикация задержки на вход или выход отключается при нажатии на любую кнопку на клавиатуре.

В отличие от светодиода «Охрана», который индицирует только задержку на выход, звуковой извещатель, встроенный в клавиатуру K16-LCD, индицирует и задержку на выход, и задержку на вход.

2.2.4 Экранная индикация

Клавиатура K16-LCD снабжена двухстрочным жидкокристаллическим индикатором, в каждой строке которого может быть отображено до 16 алфавитно-цифровых символов.

Информация, которая отображается на экране клавиатуры K16-LCD, зависит от текущего состояния прибора, а также от операций, которые выполняет пользователь.

Дежурная индикация – прибор полностью снят с охраны

Если все разделы прибора сняты с охраны и пользователей не выполняет никаких операций с клавиатурой, то на экране клавиатуры отображается текущая дата и текущее время, а также информация о текущих неисправностях прибора, если они есть.

Информация о текущей дате и времени отображается в первой строке экрана.

Информация об имеющихся неисправностях отображается во второй строке экрана.

Пример дежурного экрана клавиатуры, когда прибор полностью снят с охраны:

12.02.2015 10:25
220В НЕ ПОДКЛЮЧ.

Если в приборе имеется несколько неисправностей, то на экране клавиатуры отображается только одна, самая приоритетная.

Перечень неисправностей (перечислены в порядке приоритета при отображении):

Неисправность	Описание
ОПЛАТИТЬ ОХРАНУ!	Строка отображается в том случае, если в настройках объекта, которые выполняются в программном обеспечении «Центр охраны», выставлено одно из значений, подразумевающих информирование пользователя контрольной панели о необходимости оплаты услуг охраны.
220В НЕ ПОДКЛЮЧ.	Строка отображается в том случае, если отсутствует основное питание прибора. При конфигурировании прибора может быть включен запрет на взятие прибора под охрану при отсутствии основного питания.

НЕТ IP-СВЯЗИ	Строка отображается при отсутствии IP-подключения (по Ethernet или GPRS) к «Центру охраны». При конфигурировании прибора может быть включен запрет на взятие прибора под охрану при отсутствии IP-связи с «Центром охраны».
КОРПУС ОТКРЫТ!	Строка отображается, если корпус прибора открыт.
ЗОНА NN НЕИСПРАВ	Строка отображается, если в проводном или беспроводной шлейфе, подключенном к прибору, обнаружена неисправность: обрыв или короткое замыкание в шлейфе, отсутствие связи с беспроводным устройством, разряд источника питания беспроводного устройства и т.д.
АКБ НЕ ПОДКЛЮЧЕНА	Строка отображается, если источник резервного питания не подключен к прибору.
АКБ РАЗРЯЖЕНА	Строка отображается, если значение напряжения, измеренное на клеммах для подключения источника резервного питания, свидетельствует о том, что источник резервного питания разряжен.

Дежурная индикация – прибор частично взят под охрану

Если часть разделов прибора взята под охрану, а часть – снята с охраны и пользователь не выполняет никаких операций с клавиатурой, то на экране клавиатуры отображается текущее время, а также список разделов, взятых под охрану.

Информация о наличии разделов, взятых под охрану, и текущее время отображаются в первой строке экрана.

Список номеров разделов, взятых под охрану, отображается во второй строке экрана.

Пример дежурного экрана клавиатуры, когда прибор частично взят под охрану:

ВЗЯТ 10:25
РАЗДЕЛЫ 1,4,5

Дежурная индикация – прибор полностью взят под охрану

Если прибор полностью взят под охрану и пользователь не выполняет никаких операций с клавиатурой, то на экране клавиатуры отображается текущее время, а также информация о том, что прибор полностью взят под охрану.

Пример дежурного экрана клавиатуры, когда прибор полностью взят под охрану:

ВЗЯТ 10:25
ВСЕ РАЗДЕЛЫ

Если для прибора сконфигурирован только один раздел, то при его взятии под охрану строка «ВСЕ РАЗДЕЛЫ» не отображается.

Индикация взятия

Если взятие разрешено и задержки на выход нет, то в первой строке экрана клавиатуры в течение 3 секунд отображается фраза «ВЗЯТИЕ...», после чего экран клавиатуры переключается в дежурный режим, соответствующий состоянию охраны прибора.

Если есть задержка на выход, то в течение задержки на выход в первой строке экрана клавиатуры отображается фраза «ВЗЯТИЕ... NN», где NN – время в секундах, в течение которого будет продолжаться задержка на выход. Информация о времени, в течение которого будет продолжаться задержка на выход, обновляется каждую секунду.

Светодиодная, звуковая и экранная индикация задержки на выход отключается при нажатии на любую кнопку на клавиатуре.

Если в настройках объекта, которые выполняются в программном обеспечении «Центр охраны», выставлено одно из значений, подразумевающих информирование пользователя о необходимости оплаты услуг охраны во время взятия и снятия, то во второй строке экрана клавиатуры отображается фраза «ОПЛАТИТЬ ОХРАНУ!».

Пример экрана клавиатуры с индикацией взятия:

ВЗЯТИЕ... 18
ОПЛАТИТЬ ОХРАНУ!

Индикация снятия

Если снятие разрешено, то в первой строке экрана клавиатуры в течение 3 секунд отображается «СНЯТИЕ...», после чего экран клавиатуры переключается в дежурный режим, соответствующий состоянию охраны прибора.

Если в настройках объекта, которые выполняются в программном обеспечении «Центр охраны», выставлено одно из значений, подразумевающих информирование пользователя о необходимости оплаты услуг охраны во время взятия и снятия, то во второй строке экрана клавиатуры отображается фраза «ОПЛАТИТЬ ОХРАНУ!».

Пример экрана клавиатуры с индикацией снятия:

СНЯТИЕ...

Индикация отказа от взятия

Если при взятии под охрану будет обнаружена причина, по которой взятие под охрану невозможно, то на экране клавиатуры отображается информация об отказе от взятия, а кроме того, отображается причина отказа.

Кроме того, для индикации отказа от взятия используется звуковая индикация: четыре одиночных звуковых сигнала.

В первой строке экрана клавиатуры отображается фраза «ОТКАЗ ОТ ВЗЯТИЯ».

Во второй строке экрана клавиатуры отображается одна возможных причин отказа от взятия:

- ОПЛАТИТЬ ОХРАНУ!
- 220В НЕ ПОДКЛЮЧ.
- НЕТ IP-СВЯЗИ
- КОРПУС ОТКРЫТ!
- ЗОНА NN НЕИСПРАВ
- ЗОНА NN ТРЕВОГА

Соответствие фраз, отображаемых при отказе от взятия, причинам, вызвавшим отказ, приведено выше.

Экранная индикация отказа от взятия отображается в течение 5 секунд, после чего экран клавиатуры переключается в дежурный режим, соответствующий состоянию охраны прибора.

2.3 Teclado inalámbrico CN-K

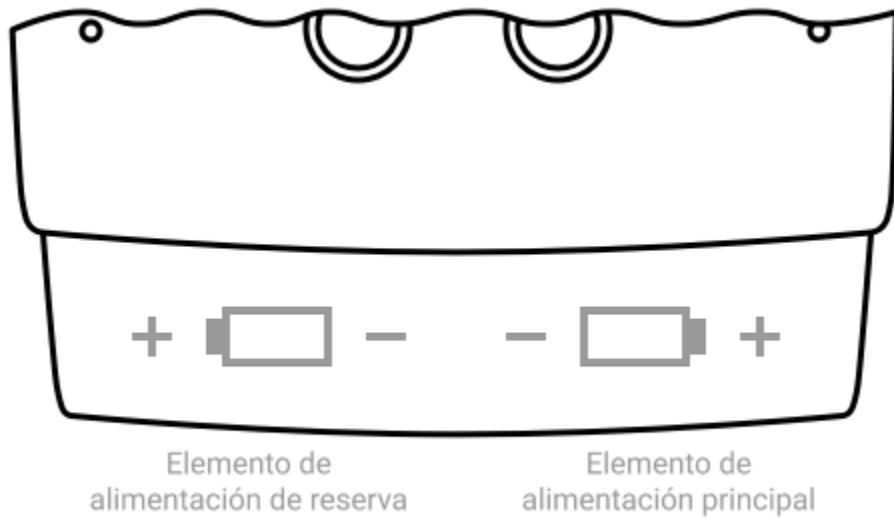


Puc. 8: Teclado CN-K

El equipo se puede controlar o informarse sobre su estado a través del teclado inalámbrico “CN-K”. El teclado se conecta al equipo “Nord GSM” a través del expansor “CN-Rasio”. Para añadir el teclado a la configuración del equipo hay que realizar las siguientes acciones:

- Quitar la tapa del teclado.
- Conectar la alimentación - la alimentación del teclado se realiza a través de dos baterías de litio de tipo CR123A (principal y de reserva). Para cambiar las baterías hay que abrir la tapa de la sección de baterías, instalar primero la batería de reserva y a continuación la principal.
- En el configurador del equipo ir a la pestaña «Dispositivos inalámbricos» y pulsar el botón “Añadir dispositivo inalámbrico”.
- Cambiar el teclado al modo “Unión”. Para ello hay que cruzar los contactos “Reseteo”, ubicados en la placa del dispositivo. Mediante destellos del LED verde, “CN-K” confirmará el cambio al modo de “Unión”.

(Más información en el apartado 5.3. «Dispositivos inalámbricos»)



Puc. 9: Sección de baterías del teclado CN-K

Al equipo se puede conectar un máximo de cuatro teclados inalámbricos, teniendo en cuenta que el equipo puede funcionar con todos los teclados al mismo tiempo.

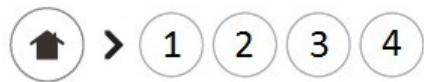
2.3.1 Arme y desarme

En el equipo está realizada la posibilidad de arme y desarme del sistema de seguridad de varias particiones con un código de usuario. El ajuste de particiones que pueden ser armadas o desarmadas con un código en concreto, se realiza al realizar la configuración del equipo.

Arme del sistema de seguridad

Para armar la partición hay que pulsar “casita” e introducir el código del usuario.

- si el código es correcto, el sistema de seguridad del objeto (partición) será armado, el teclado confirmará el arme mediante la activación del LED rojo. O se activará la cuenta del intervalo de retraso de salida que va acompañada por una indicación acústica o LED.
- si el código es incorrecto o al usuario al que le pertenece ese código, le corresponde más de una partición, el teclado mostrará un error.
- si el arme del sistema de seguridad no es posible, el teclado mostrará un error.



Puc. 10

Si al código de usuario están asignadas varias particiones, primero el usuario debe pulsar el botón “casita”, elegir el apartado, cuyo estado desea cambiar y a continuación teclear el código.



Puc. 11: Ejemplo de arme de la partición №1 con el código 1234

Denegación del arme del sistema de seguridad

La “Denegación del arme” - es la imposibilidad de armar el sistema de seguridad del objeto, si la alarma de seguridad en el objeto no funciona correctamente, o si el arme del sistema de seguridad está prohibido por el impago de los servicios de seguridad.

Están previstos los siguientes motivos de denegación del arme:

- fallo de una o varias zonas;
- alarma en una o varias zonas;
- ausencia de comunicación con el programa de la consola por el canal IP;
- ausencia de 220 V en el objeto;
- impago de los servicios de seguridad;
- está abierto el cuerpo del equipo.

Desarme del sistema de seguridad

Si el usuario puede controlar sólo una partición, para desarmar el sistema de seguridad hay que introducir el código del usuario.

- si el código es correcto, el sistema de seguridad del objeto (partición) será desarmado. El teclado confirmará el desarme mediante la activación del LED verde.
- si el código es incorrecto o el usuario al que le pertenece ese código puede controlar varias particiones, el teclado mostrará un error.



Puc. 12

Si el usuario puede controlar varias particiones, para desarmar el sistema de seguridad hay que teclear el número de la partición y a continuación # e introducir el código del usuario.

- Si el código es correcto, el sistema de seguridad de la partición será desarmado. El teclado confirmará el desarme mediante la activación del LED verde.
- Si se vuelve a desarmar el sistema de seguridad de la misma partición, el teclado mostrará su estado: se encenderá el LED verde.



Puc. 13: Ejemplo de desarme de la partición №1 con el código 1234

La cuenta del intervalo de retraso de entrada o intervalo de retraso de salida se indica mediante un sonido intermitente que se reproduce durante todo el intervalo de retraso. La indicación acústica de retraso de entrada o salida se desconecta al pulsar cualquier botón del teclado.

2.3.2 Recepción del estado

En el teclado “CN-K” hay un LED verde y uno rojo:

- El LED rojo se enciende al armar la partición.
- Al desarmar la partición se enciende el LED verde.
- Los LEDs rojo y verde parpadean simultáneamente si se produjo un error. Por ejemplo, al introducir un código incorrecto del usuario o en caso de denegación del arme.

Recepción del estado del objeto

Para recibir la información sobre el estado del objeto hay que pulsar el botón **i**:

- si todas las particiones del equipo están desarmadas, se encenderá el LED verde;
- si una parte de las particiones está armada y una parte está desarmada, el teclado mostrará un error, ya que hay que indicar expresamente el número de la partición cuyo estado hay que recibir;
- si en la configuración del equipo no hay ninguna partición, el equipo mostrará un error;

Recepción del estado de la partición

Para recibir la información sobre el estado de la partición hay que pulsar el botón del número de la partición y el botón **i**:

- si la partición está armada, se encenderá el LED rojo;
- si la partición está desarmada, se encenderá el LED verde;
- si en la configuración del equipo no existe una partición con tal número, se indicará un error.

2.3.3 Botón de emergencia

Si en la configuración del equipo está permitido el uso del teclado en calidad de botón de emergencia, para la activación hay que pulsar y mantener pulsados durante 3 segundos los botones de las “casitas”. La activación de los LEDs verde y rojo durante 1 segundo acompañada con sonido confirma que fue pulsando el botón de emergencia.

Si en la configuración del equipo está prohibido el uso del teclado en calidad de botón de emergencia, el teclado mostrará un error.

2.3.4 Desactivación de la iluminación y el sonido

En el teclado “CN-K” existe la posibilidad de activación y desactivación del sonido y la iluminación.

Para activar o desactivar el sonido de confirmación de pulsación de las teclas, al mismo tiempo hay que pulsar y mantener pulsadas las teclas «#» y «9». Para la activación y la desactivación de la iluminación, al mismo tiempo hay que pulsar y mantener pulsadas las teclas «#» y «0».

2.4 Llavero inalámbrico

El llavero inalámbrico así como la llave - TM se vinculan al usuario. Mediante el llavero se puede armar o desarmar el sistema de seguridad de una partición. Si el usuario desea tener la posibilidad de armar o desarmar varias particiones al mismo tiempo, hay que configurar las correspondientes reglas en el apartado “Sistema automático”.

El llavero dispone de un botón de alarma de emergencia, que una vez pulsado hará que el equipo cree un evento de emergencia.

2.5 Aplicación móvil MyAlarm

MyAlarm – es una aplicación móvil para el trabajo con sistemas de seguridad de alarma.

La aplicación MyAlarm sólo está disponible para los clientes de la empresa de seguridad.

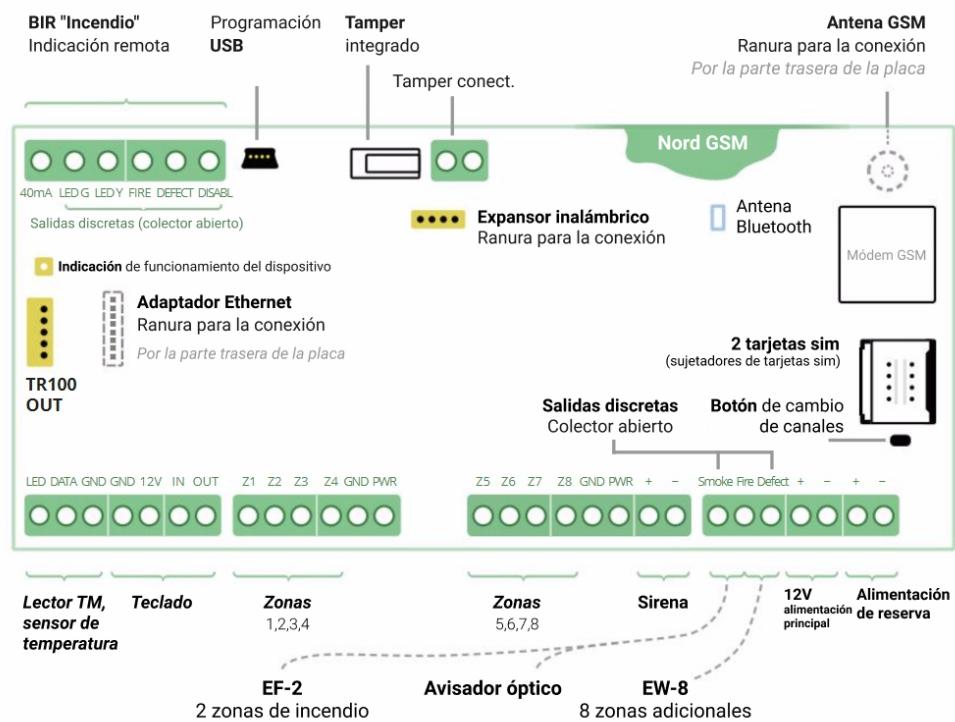
Mediante la aplicación móvil se puede controlar el estado de los equipos “Nord GSM”, que funcionan a través de GPRS o Ethernet. Para ello hay que concederle a la persona responsable el acceso al objeto en el software “Security Center”.

Para armar o desarmar desde la aplicación hay que pulsar el ícono con la imagen de un candado. A continuación hay que introducir el código del usuario. Podrá encontrar una información más detallada en el apartado en el sitio de soporte técnico.

- MyAlarm Android
- MyAlarm iOS

3 Montaje y primera puesta en marcha

3.1 Esquema de montaje del equipo



Puc. 14

3.2 Conexión de zonas por cable

Los cables de señal de las zonas se conectan a los bornes «Z1»–«Z8».

Los cables comunes de las zonas se conectan a los bornes «GND».

Los cables positivos de alimentación de las zonas de seguridad (12 V) se conectan a los bornes “PWR”.

Los cables positivos de alimentación de las zonas de incendio (12 V) se conectan al borne “SMOKE”.

3.2.1 Zona normal cerrada y normal abierta

El estado normal de la zona se determina por los avisadores que están incluidos en la misma:

- si el estado normal para la zona está determinado como cerrado, en tal zona deben usarse avisadores que también disponen de contactos cerrados de su relé de salida en estado normal. En caso de alarma tales avisadores deben abrir los contactos del relé de salida;
- si el estado normal para la zona está determinado como abierto, en tal zona deben usarse avisadores que disponen de contactos abiertos de su relé de salida en estado normal. En caso de alarma tales avisadores deben cerrar los contactos del relé de salida.

Hay que destacar que la gran mayoría de los avisadores infrarrojos y de contacto magnético modernos disponen de contactos normalmente cerrados de su relé de salida. De esta forma, para las zonas en las cuales se incluyen estos avisadores, el estado normal debe determinarse como cerrado.

Los avisadores normalmente abiertos se conectan a la zona en paralelo y los normalmente cerrados - en serie.

En una zona se pueden conectar avisadores sólo de un tipo: o normalmente cerrados, o normalmente abiertos.

3.2.2 Resistencias terminales

Si al conectar la zona no se usan resistencias terminales, para tal zona el equipo puede determinar sólo uno de dos estados: “Alarma” o “Norma”. Tal zona es muy vulnerable: si el estado normal para la zona se determina como abierto, es suficiente simplemente con cortar el cable de la zona en cualquier lugar accesible, y la zona para siempre se quedará en estado normal, en tal zona nunca se producirá una alarma. Nada mejor será una zona cuyo estado normal está determinado como cerrado: si se consigue cerrar los cables de alarma de la zona en cortocircuito, en esta zona tampoco nunca habrá una señal de alarma.

Una resistencia terminal instalada en la zona permite diferenciar un fallo en la zona de una alarma. Qué tipo de fallo puede ser determinado - ruptura o cortocircuito - depende del estado normal de la zona: para el estado normal de la zona abierta una resistencia terminal permite determinar la ruptura de la zona y para el estado normal cerrada - cortocircuito.

Dos resistencias terminales permite determinar la ruptura y el cortocircuito para la zona con cualquier estado normal.

Para minimizar los fallos de las zonas de alarma, se recomienda conectar a las zonas como mínimo una resistencia terminal.

3.2.3 Zona sin resistencias terminales

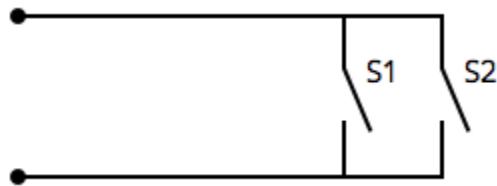


Рис. 15: Нормально разомкнутый шлейф

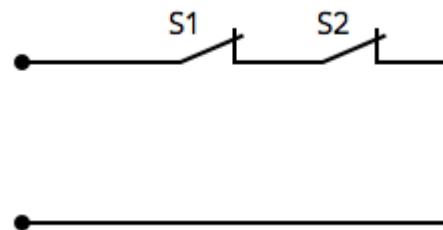


Рис. 16: Нормально замкнутый шлейф

3.2.4 Zona con una resistencia terminal

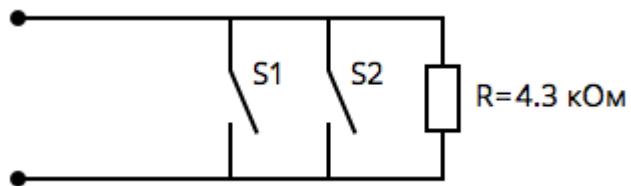


Рис. 17: Нормально разомкнутый шлейф

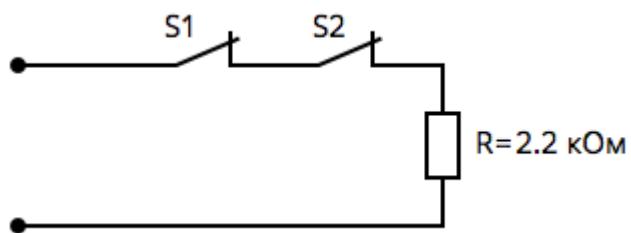


Рис. 18: Нормально замкнутый шлейф

3.2.5 Zona con dos resistencias terminales

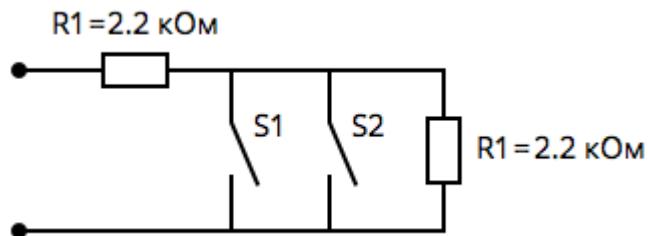


Рис. 19: Нормально разомкнутый шлейф

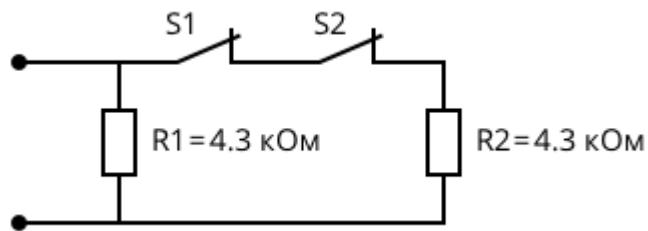


Рис. 20: Нормально замкнутый шлейф

3.2.6 Zonas por cable en el configurador

Al realizar la configuración del equipo hay que especificar expresamente la norma para la zona por cable, así como la cantidad de resistencias terminales. Se puede hacer en la pestaña “[Zonas](#)”.

3.3 Conexión de avisadores de incendio

3.3.1 Avisadores de incendio de cuatro cables

Los cables de señal, a los cuales están conectados los avisadores de incendio de cuatro cables se conectan a los bornes «Z1»–«Z8».

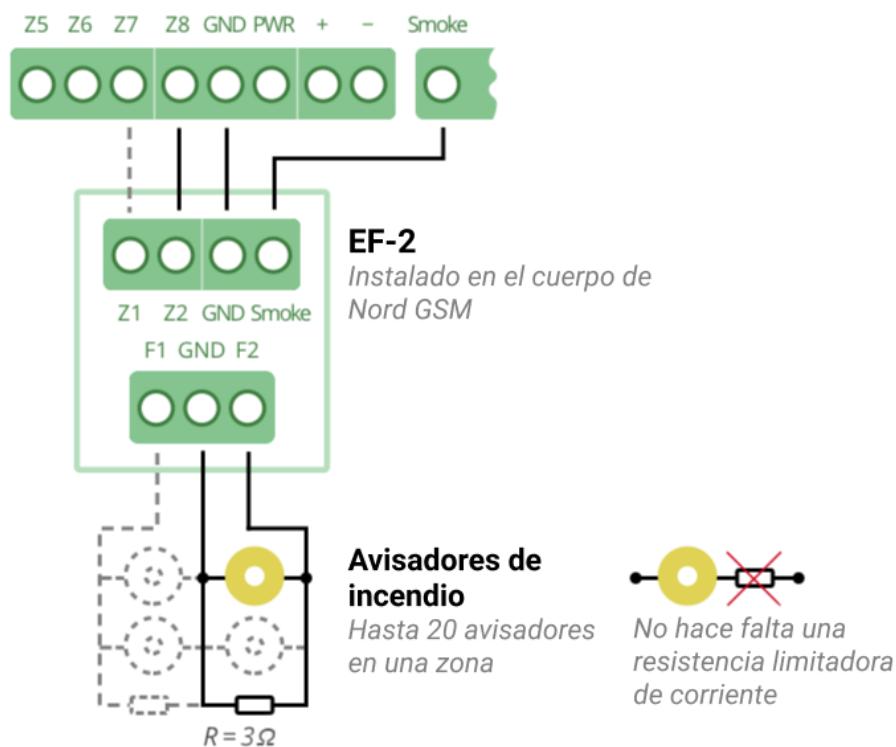
Los cables comunes de las zonas se conectan a los bornes «GND».

Si hay que resetear la alimentación de los avisadores de incendio después de la alarma, el cable positivo de alimentación de la zona hay que conectarlo al borne SMOKE. En este caso, después de finalizar el intervalo de repetición de alarmas (ver apartado “Configuración”) en la alimentación de los sensores se producirán desconexiones a corto plazo.

Si no se requiere el reseteo de la alimentación de los avisadores de incendio, hay que conectar el cable positivo de alimentación de la zona de incendio al borne PWR.

3.3.2 Avisadores de incendio de dos cables

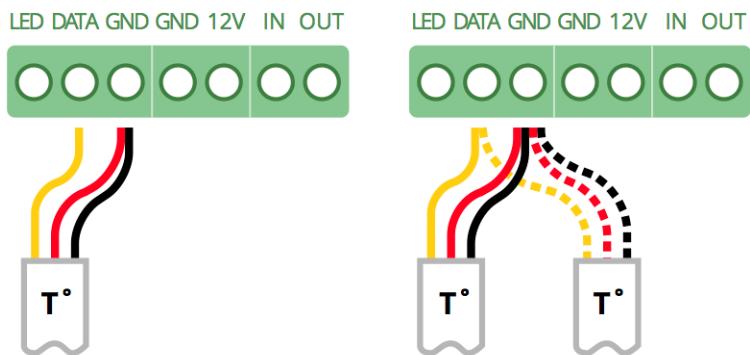
Los avisadores de incendio de humo de dos cables se conectan al equipo sólo a través del dispositivo de coordinación “EF-2”, que permite conectar avisadores de dos cables por un esquema de cuatro cables.



Puc. 21: Esquema de conexión de avisadores de incendio de humo de dos cables a través del EF-2

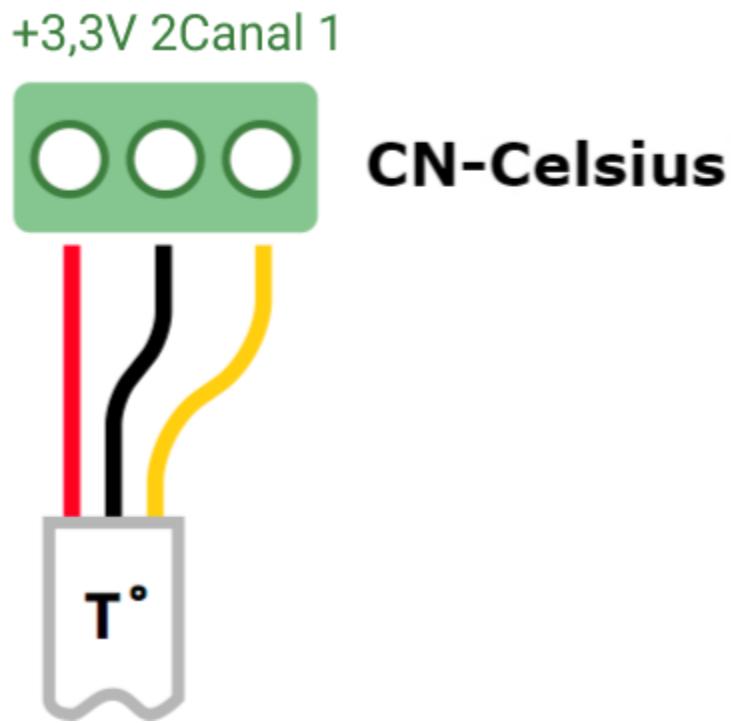
3.4 Conexión de sensores de temperatura

El sensor de temperatura por cable se conecta al grupo de los bornes “Lector”. Los cables negro y rojo que provienen del sensor, deben estar torcidos juntos y conectados al borne “GND” y el cable amarillo al borne “DATA” - tal como se indica en la imagen de abajo. Si hay que conectar varios sensores por cable al mismo tiempo, todos ellos deben conectarse de forma paralela el uno al otro. Para que el equipo pueda detectar el sensor de temperatura por cable, en la configuración del equipo hay que activar el modo de solicitud continua de la interfaz 1-Wire. Esto se puede hacer en la pestaña “Varios” en el apartado “Control e indicación”.



Puc. 22: Esquema de conexión del sensor de temperatura por cable al equipo

Al sensor de temperatura inalámbrico CN-Celsius se puede conectar un sensor por cable.



Puc. 23: Esquema de conexión del sensor de temperatura por cable al CN-Celsius

3.5 Conexión del expansor “EW-12”

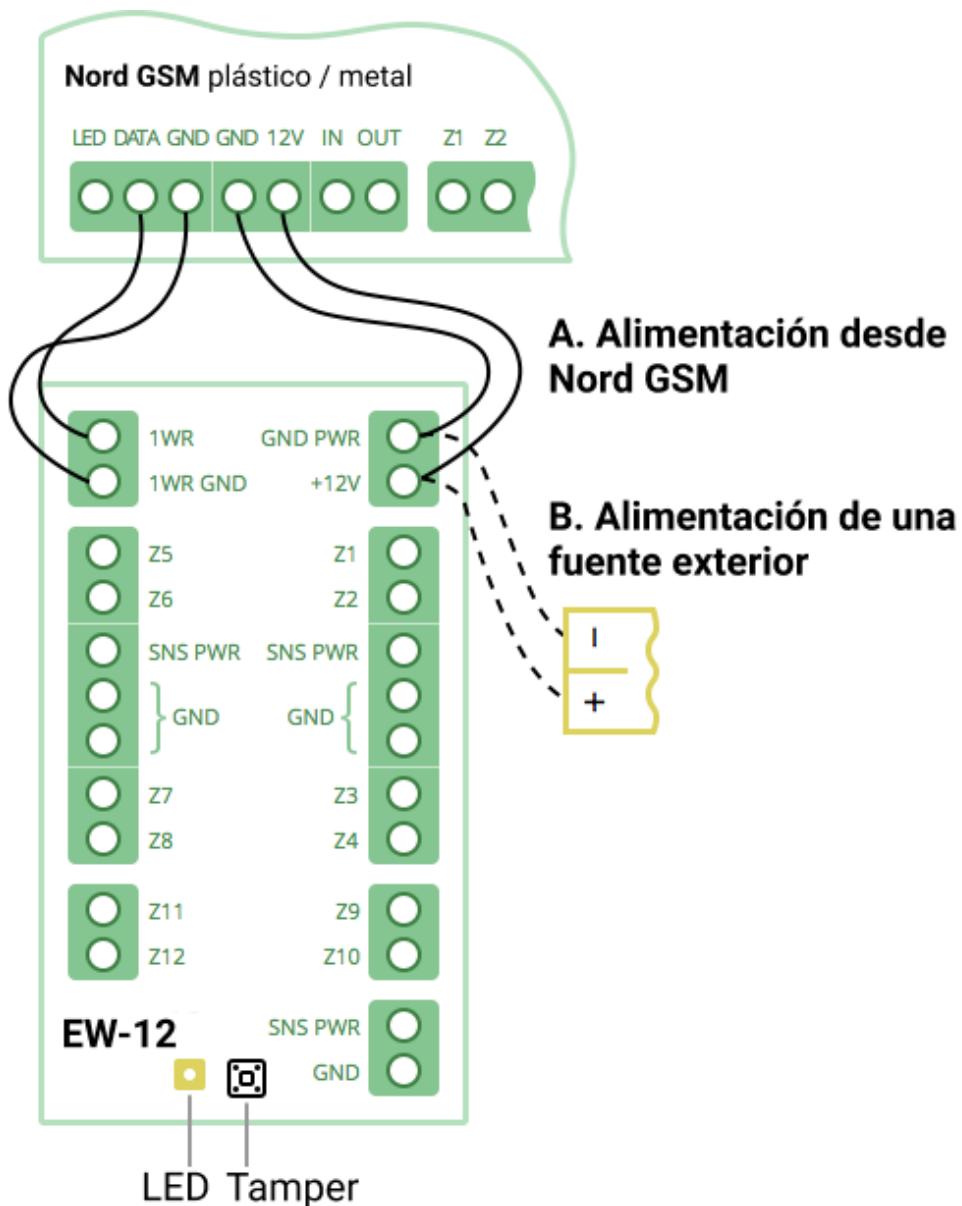
“EW-12” - expansor de zonas por cable para paneles de control “Nord GSM”, con su ayuda se puede aumentar la cantidad de zonas hasta 16 o la cantidad de salidas tipo “colector abierto”.



Puc. 24: EW-12

Conexión al equipo

El expansor se conecta al equipo al grupo de bornes “Lector”, situado en la parte izquierda de la línea de bornes del equipo: el borne “1WR” del expansor se conectan al borne “DATA” del equipo y el borne “1WR GND” del expansor - al borne “GND” del equipo.



Puc. 25: Esquema de conexión del "EW-12" al equipo

Si el expansor está conectado correctamente, el LED del expansor debe parpadear, las zonas aparecerán en el configurador automáticamente en la pestaña **Zonas**.

Alimentación del expansor

Para conectar la alimentación del expansor sirven los bornes con el marcaje “GND PWR” y «+12V».

La alimentación puede suministrarse de dos formas:

- Del equipo mismo, pero con ello hay que tener en cuenta que la carga máxima es de 200 mA.
- De la fuente de alimentación ininterrumpida.

Conexión de zonas al expansor

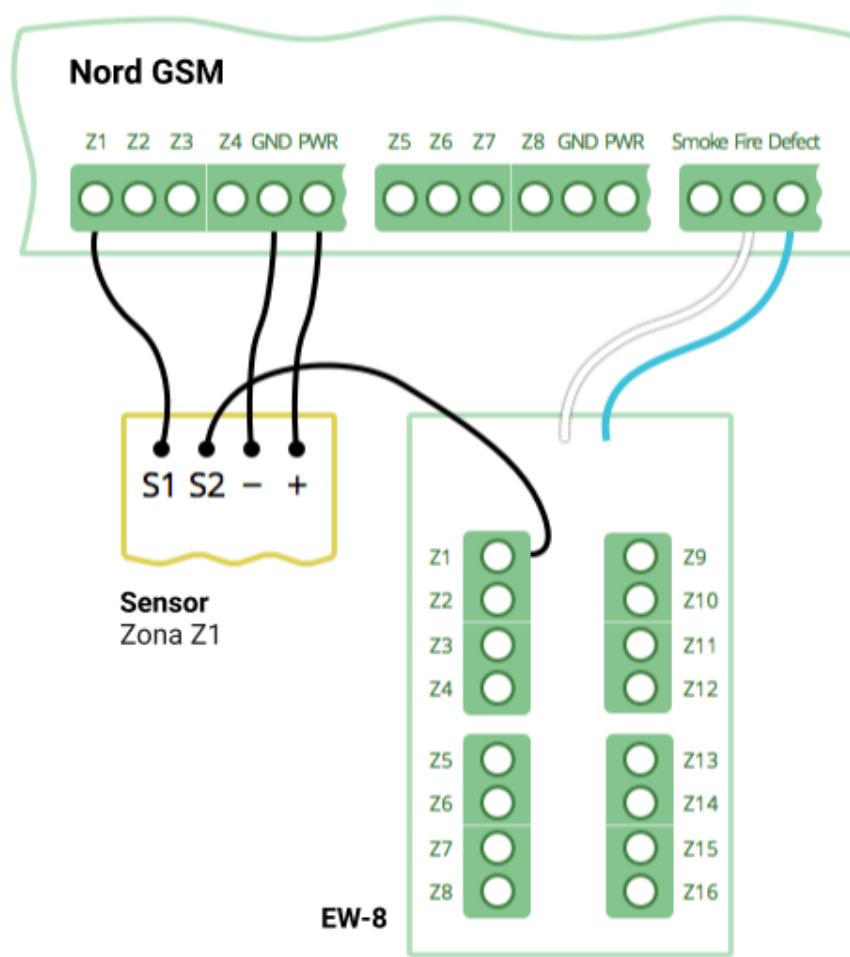
Los bornes «Z1» – «Z8» sirven para la conexión del cable de señal de las zonas. Los bornes «GND» - para la conexión del cable “negativo” de alimentación de las zonas y el segundo cable de señal de las zonas. Los bornes «SNS PWR» sirven para la conexión del cable “positivo” de alimentación de las zonas.

Al igual que en el equipo mismo, en el expensor en cada una de las zonas se pueden conectar hasta dos resistencias. Los nominales de las resistencias y los esquemas de conexión de las zonas se muestran en el apartado Conexión de zonas por cable.

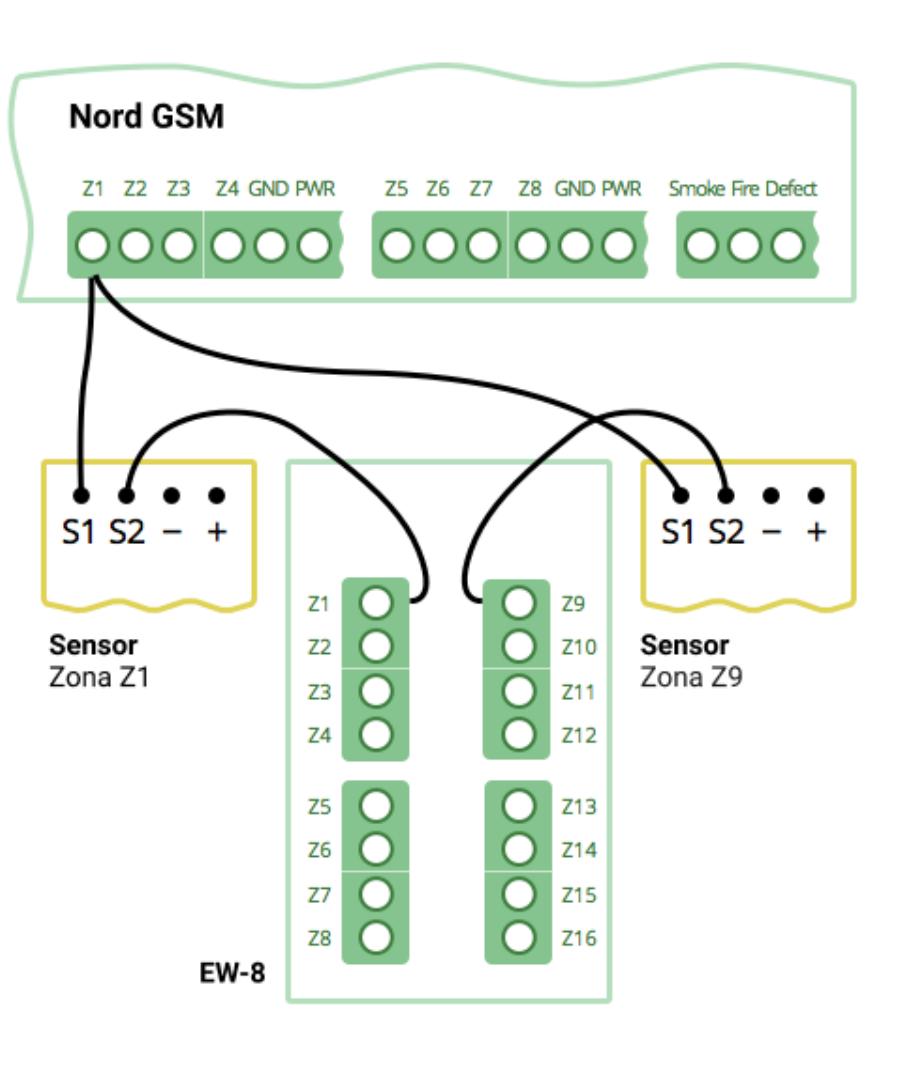
Cada borne «Z1» – «Z8» puede ser una zona o salida de tipo “colector abierto”, esto se indica al configurar el panel de control:

- Si en el configurador la zona está desconectada, se puede usar como colector abierto.
- Si en el configurador la zona está conectada, no se puede usar como colector.

3.6 Conexión del expansor “EW-8”



Puc. 26: Esquema de conexión del EW-8 al equipo



Puc. 27: Esquema de conexión de dos zonas a través del EW-8

3.7 Configuración del canal GSM

El equipo dispone de un modem GSM integrado que puede funcionar por turno con una de las dos tarjetas SIM instaladas.

3.7.1 Instalación de tarjetas SIM

El sujetador para tarjetas SIM se sitúa en la parte derecha de la placa del equipo.

Debajo se sitúa la tarjeta SIM principal (SIM1), arriba - la de reserva (SIM2). Las tarjetas SIM se instalan en el sujetador con la superficie de contacto de cara a la placa. Antes de instalar las tarjetas SIM en el equipo, corte por completo el suministro de corriente hacia el dispositivo, de lo contrario la tarjeta SIM puede estropearse con electricidad estática.

No se olvide desactivar la solicitud del código PIN. Si no desconecta el código PIN: en primer lugar, el equipo no podrá usar la correspondiente tarjeta SIM; en segundo lugar, la tarjeta SIM puede bloquearse después de varios intentos de activación.

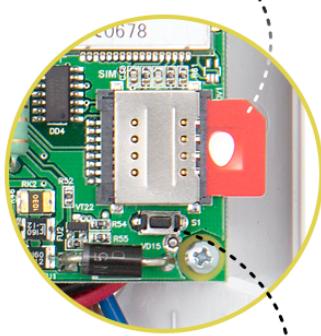
Si usa sólo una tarjeta SIM, es imprescindible que la instale en la ranura para la tarjeta SIM principal - más cerca de la placa.

3.7.2 Verificación del nivel de la señal GSM

Antes de empezar a usar el equipo es imprescindible verificar el nivel de señal en el lugar donde se tiene previsto instalar el equipo. Esto se puede hacer mediante el LED HL1 que se encuentra en la parte izquierda de la placa del equipo o mediante la pestaña Panel del estado del configurador Hubble. Podrá encontrar más información sobre la verificación de los canales de comunicación en el apartado 5.14.

Si el nivel de la señal GSM es malo hay que ubicar el equipo en otro lugar o instalar una antena GSM remota.

Below - main SIM;
above - backup SIM;



Switching channel button

3.7.3 Conexión de la antena GSM remota

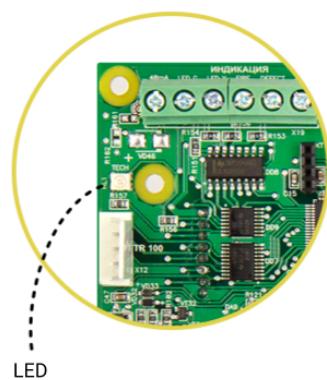
Para conectar la antena remota en vez de la antena interna, hay que realizar las siguientes acciones por orden:

- sacar la placa del equipo del cuerpo, desatornillando los tornillos de fijación;
- cambiar la antena interna por una remota;
- comprobar que la placa con la antena remota instalada está bien pegada a los soportes de fijación;
- en caso de necesidad taladrar en el cuerpo un orificio con un diámetro de 10 mm, para sacar el alimentador de la antena hacia fuera. En este caso primero hay que pasar el alimentador de la antena a través del orificio en el cuerpo y sólo después enrosarlo al conector en la placa;
- instalar la placa en el cuerpo, atornillando los tornillos de fijación.

Antes de fijar finalmente la antena externa en su lugar fijo de instalación, es imprescindible verificar el nivel de la señal en ambas SIM en el lugar dado concreto. Si el nivel de la señal no es satisfactorio, hay que ubicar la antena en otro sitio.

Recomendaciones de instalación de la antena externa:

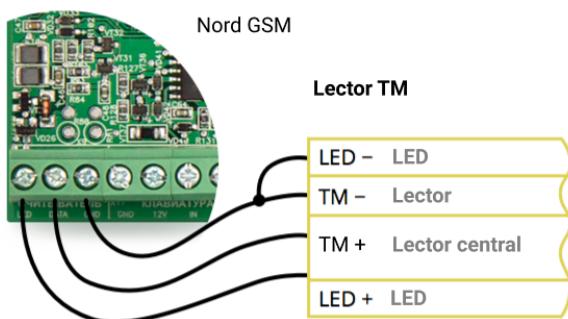
- alejar del equipo a una distancia no menos de 50 cm;
- no enrollar el alimentador de la antena;
- fijar la antena sobre una superficie dieléctrica;
- fijar la antena en posición vertical.



3.8 Conexión del lector Touch Memory

El equipo dispone de una interfaz integrada para la conexión de lectores de llaves TM. Al equipo se pueden añadir hasta 32 llaves TM.

El lector Toch Memory se conecta al equipo en los bornes LED, DATA y GND del grupo “Lector”.



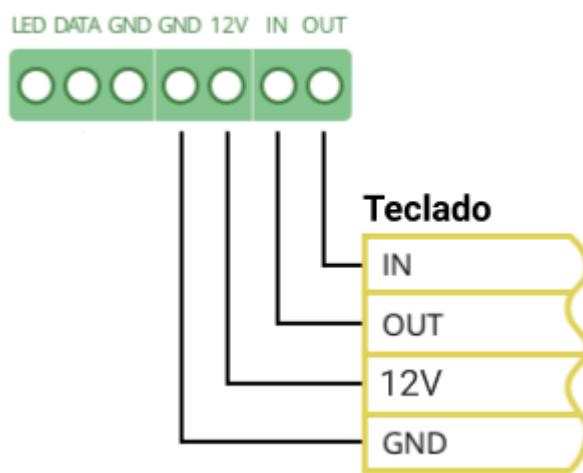
Puc. 28: Esquema de conexión del lector Touch Memory

En vez del lector TM se puede conectar cualquier lector con emulación del protocolo Dallas Touch Memory (DS1990A). Por ejemplo, lectores Proxymity (“PS-01”, “SR-Z2B”).

Con ello, hay que tomar en consideración que para conectar algunos lectores que emulan el protocolo DS1990A, hay que desactivar el modo de solicitud continua de la interfaz 1-wire, que está activado de forma predeterminada. Para hacerlo, en el configurador hay que pasar a la pestaña **Varios** y desmarcar la casilla para el parámetro “Activar el modo de solicitud continua de la interfaz 1-Wire”.

3.9 Conexión de teclados por cable

Los teclados por cable, tales como “K16-LCD”, “K14-LED” se conectan al equipo en los bornes del grupo “Teclado”.



Puc. 29: Esquema de conexión de teclados por cable

4 Actualización del software

Antes de empezar a configurar el equipo, hay que asegurarse de que la versión del software instalada en el mismo está actualizada. Para hacerlo, hay que conectar el equipo a la computadora y ejecutar la utilidad para la actualización del firmware del equipo a través de USB.

El paquete de programas que se requieren para conectar el equipo a la computadora y realizar la actualización de la versión del software, se puede descargar desde el sitio oficial de soporte técnico de NTKF “C-Nord” (support.cnord.ru), desde la página “Файлы для загрузки”.

El paquete para la actualización de la versión del software de los equipos se suministra en forma de archivo zip con un nombre de tipo **CnordFirmware-AAAAMMDD-XX.XX.zip**, donde **AAAAMMDD** - es la fecha de realización del software y **XX.XX** es la versión del software en archivo. El contenido del archivo hay que descomprimirlo en una carpeta en el disco duro de la computadora. En el archivo se incluyen los siguientes programas:

- controlador para la conexión del equipo a la computadora; El controlador se encuentra en la carpeta **Driver**
- utilidad que sirve para la actualización de la versión del software del equipo; El archivo ejecutable de la utilidad se llama **CnordFirmware.exe**, precisamente este archivo es el que hay que ejecutar para actualizar la versión del software del equipo.

En el paquete para la actualización de la versión del software del equipo están incluidas las versiones actuales de firmwares para los siguientes dispositivos:

- «Nord GSM», «Nord GSM WRL», «Nord LAN», «Nord RF»;
- «Nord GSM Mini»;
- «Nord GSM Air»;
- «TR-100 GSM IV»;
- «Serzhant GSM»;
- «Soyuz GSM»;
- «Soyuz PCB GSM».

4.1 Conexión del equipo a la computadora

En la computadora a la cual se conecta al equipo, debe estar instalado un sistema operativo de la familia Windows (XP/7/8/10). No importa si el sistema operativo es de 32 o de 64 bits.

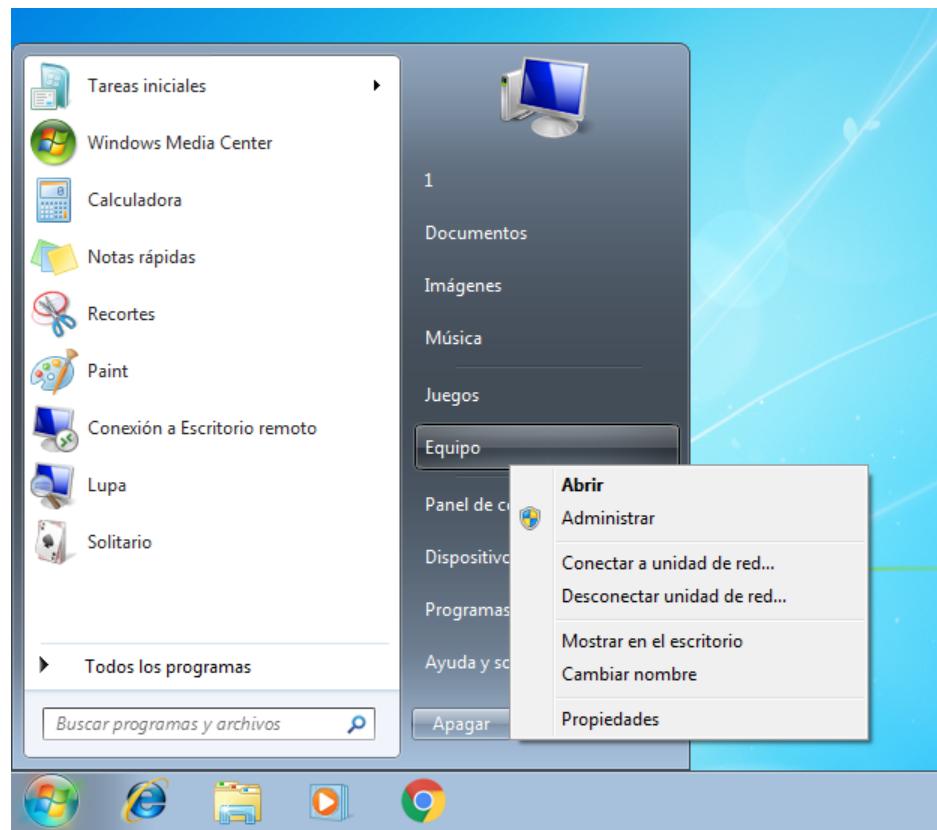
Antes de conectar el equipo a la computadora, le recomendamos *insistemente* que lo conecte a una alimentación principal o de reserva. Si el equipo se alimenta únicamente por USB, puede funcionar de forma no estable.

Antes de empezar a trabajar con el equipo, hay que instalar el controlador. El equipo se conecta a la computadora mediante un cable USB-Mini y el controlador es un software especial que le permite a los programas, con los cuales interacciona el usuario, intercambiar datos con el equipo.

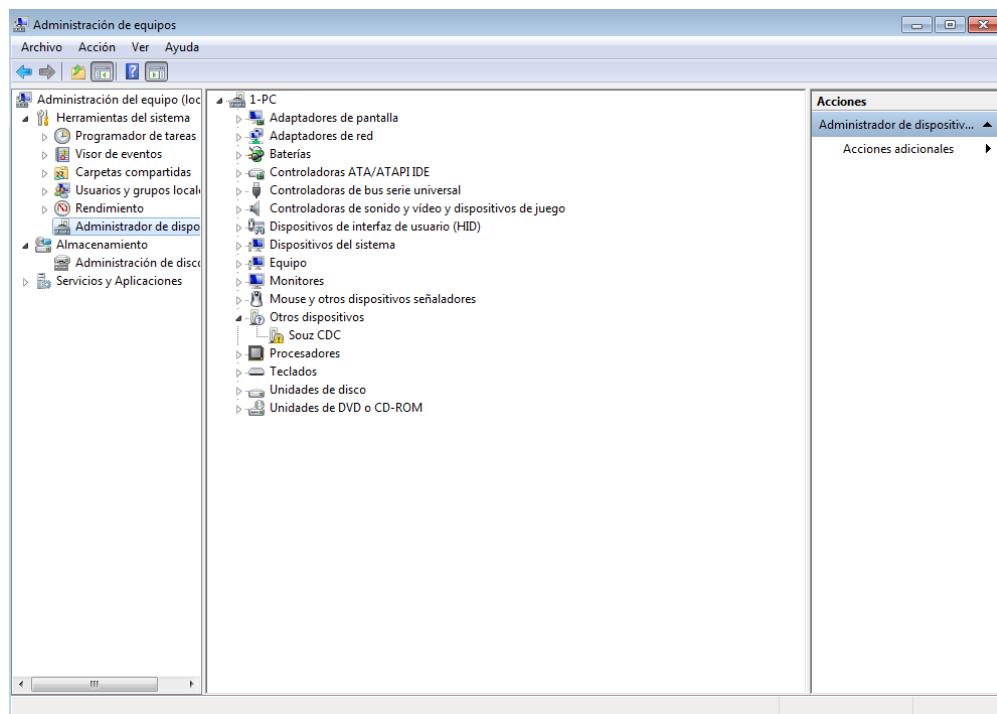
Para todos los sistemas operativos se suministra el mismo controlador.

4.2 Instalación del controlador en Windows XP y Windows 7

Durante la primera conexión del equipo a la computadora en la bandeja del sistema del panel de tareas aparecerá una notificación de que fue encontrado un dispositivo nuevo. La instalación del controlador puede realizarse a través del «Administrador de dispositivos». Para ello hay que entrar en el menú “Inicio”, pulsar el botón derecho del ratón en “Equipo” y seleccionar Administrar, a continuación en el medio de la izquierda seleccionar «Administrador de dispositivos».

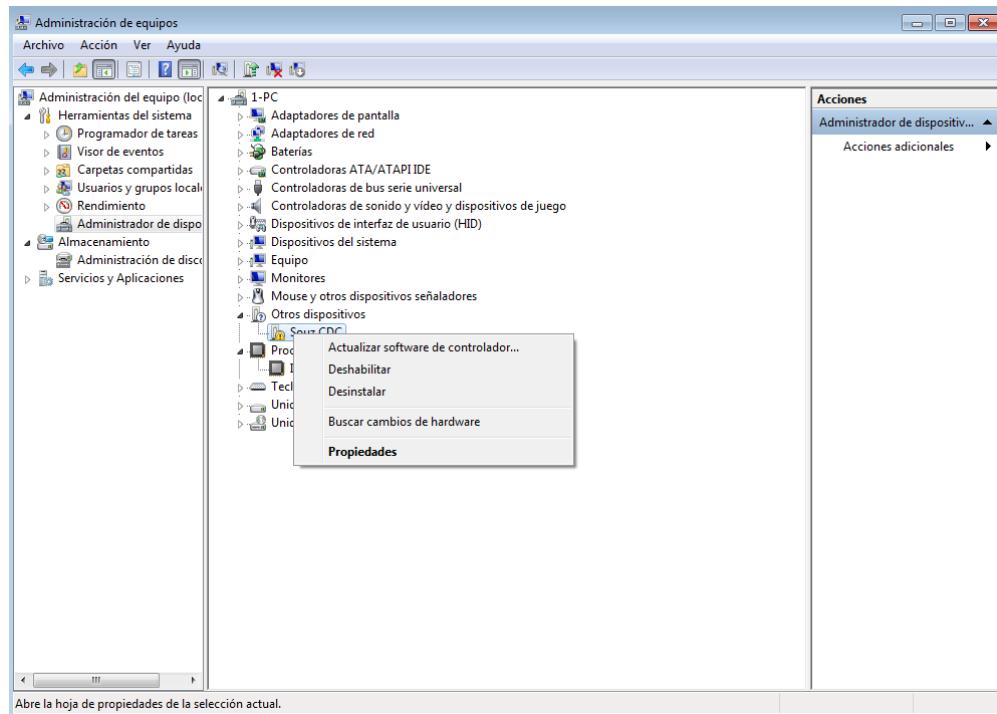


Puc. 30



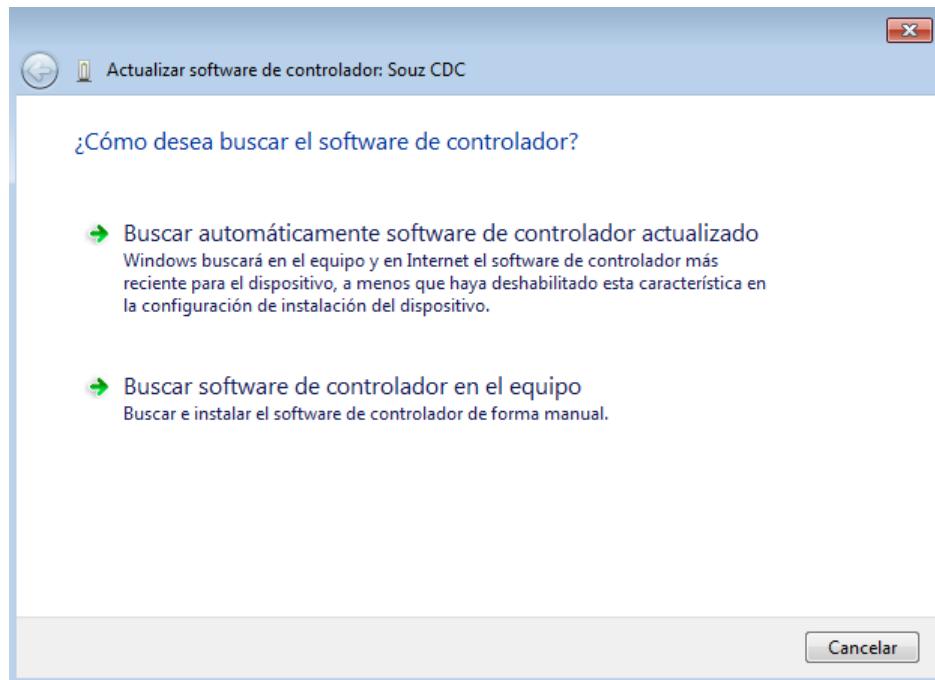
Puc. 31

Hay que pulsar el botón derecho del ratón sobre el dispositivo Soyuz CDC y seleccionar el punto del menú “Actualizar software del controlador”.



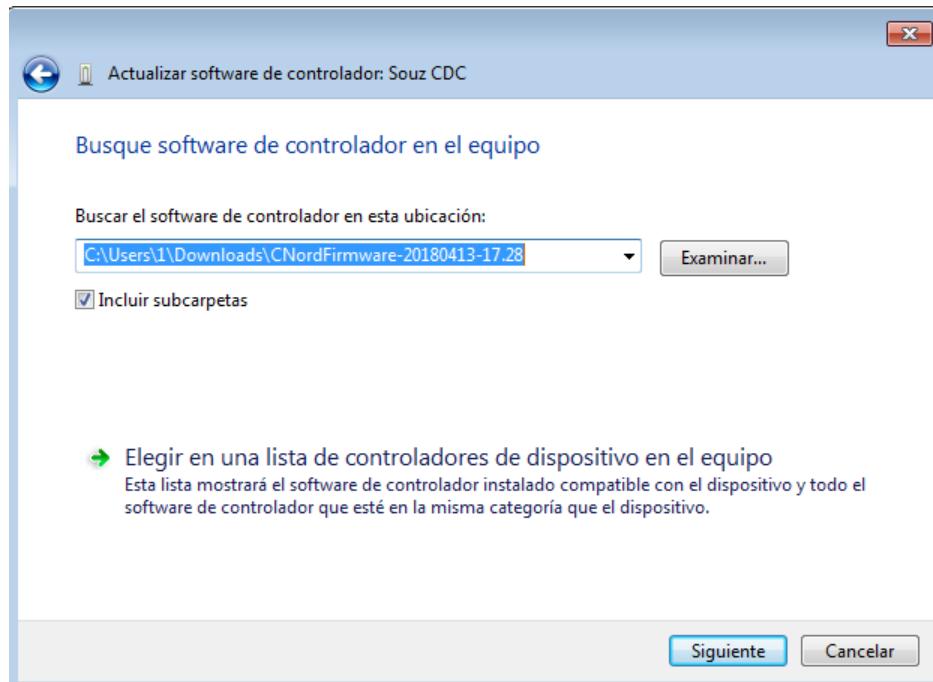
Puc. 32

Hay que renunciar a la propuesta de buscar automáticamente software del controlador actualizado para un nuevo dispositivo, seleccionando la instalación del controlador de forma manual.



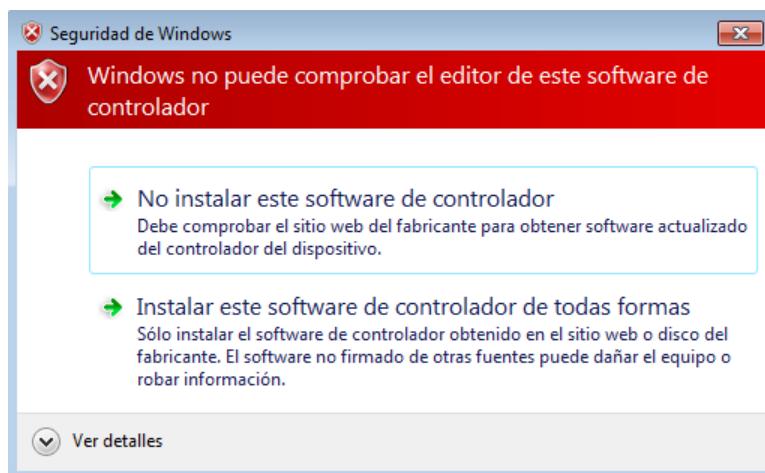
Puc. 33: Selección de instalación manual

Especificar la ruta hacia el archivo **Driver** y pulsar Siguiente.



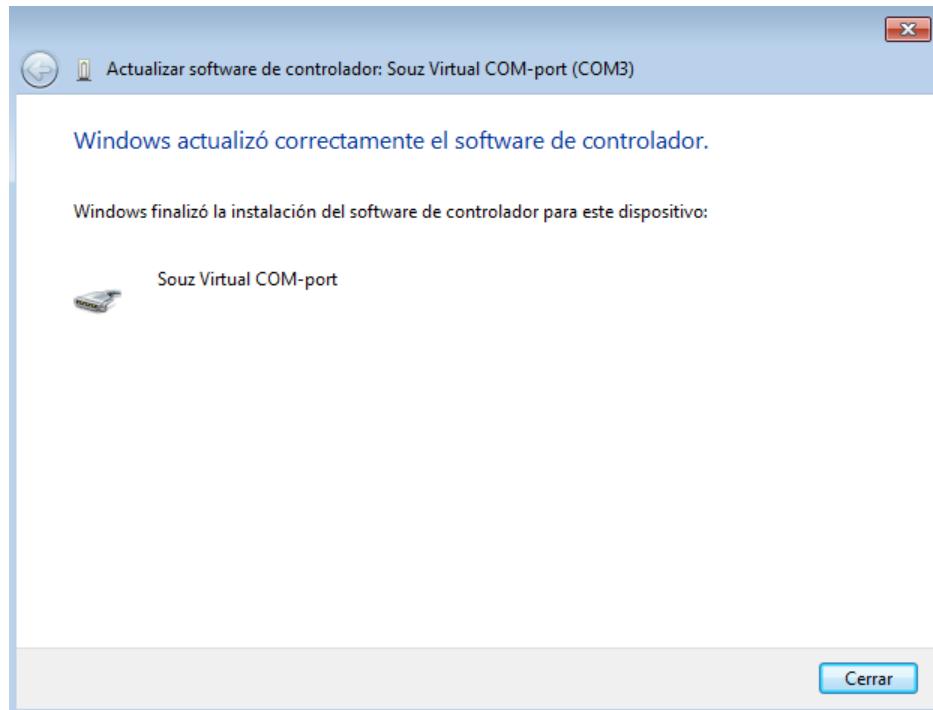
Puc. 34: Selección del lugar de búsqueda del controlador

El controlador para el equipo “Nord GSM” no tiene firma digital. Por ello hay que confirmarle expresamente al sistema operativo de que hace falta instalarlo.



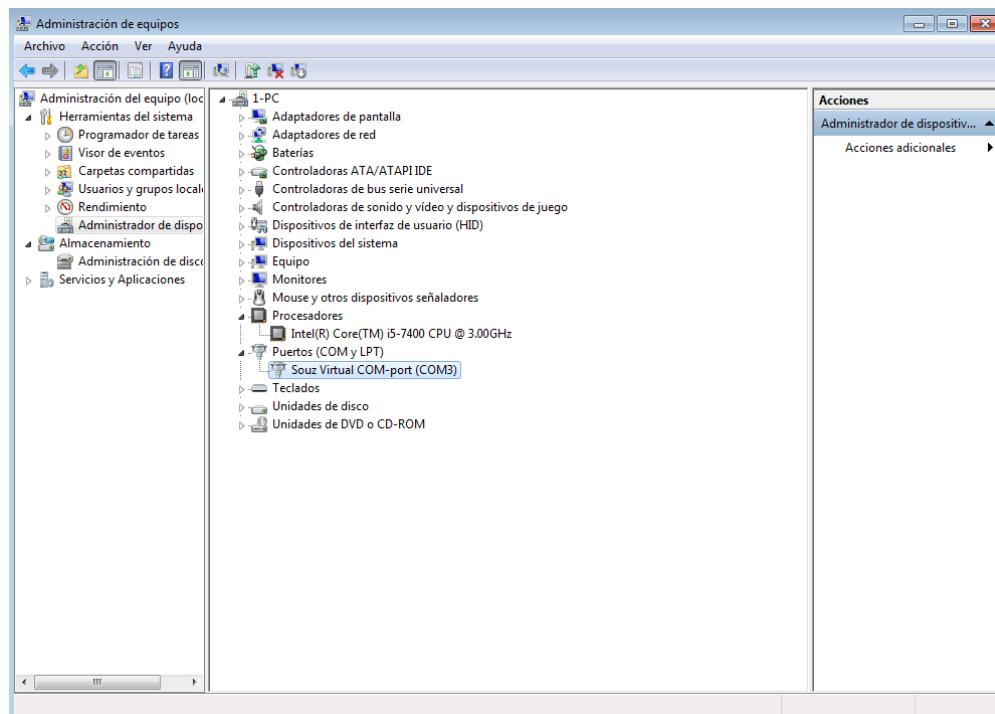
Puc. 35: Confirmar la instalación del controlador sin firma digital

Después de finalizar la instalación del controlador hay que pulsar el botón “Cerrar”.



Puc. 36: Finalización de la instalación del controlador

Para asegurarse que el controlador para el dispositivo está instalado, se puede abrir el «Administrador de dispositivos» de Windows y buscar el puerto serie virtual que corresponde al equipo conectado a la computadora.



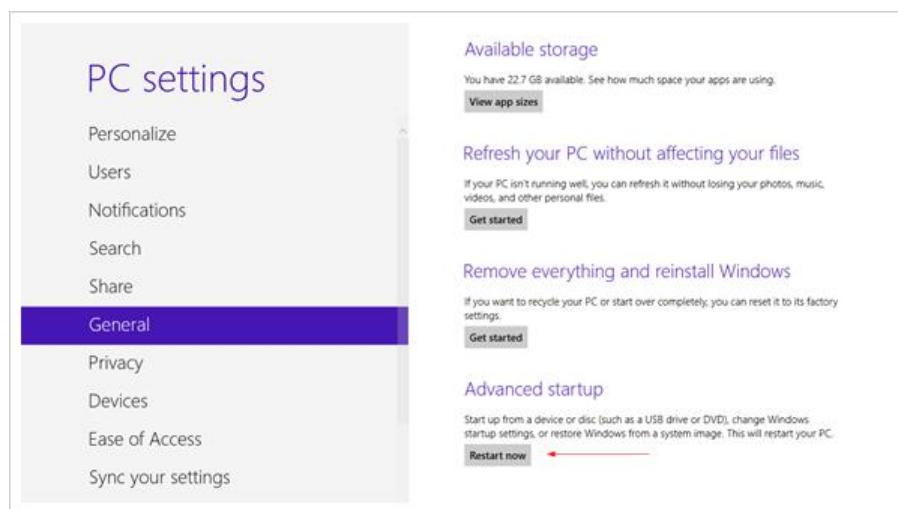
Puc. 37: Puerto serie del equipo en el «Administrador de dispositivos»

4.3 Instalación del controlador en Windows 8

El sistema operativo Windows 8 no permite instalar controladores sin firma digital, tal como era posible en las versiones anteriores. Por ello, antes de empezar a instalar los controladores del equipo en este sistema operativo, hay que iniciararlo en modo especial - con comprobación obligatoria de firma de controladores deshabilitada.

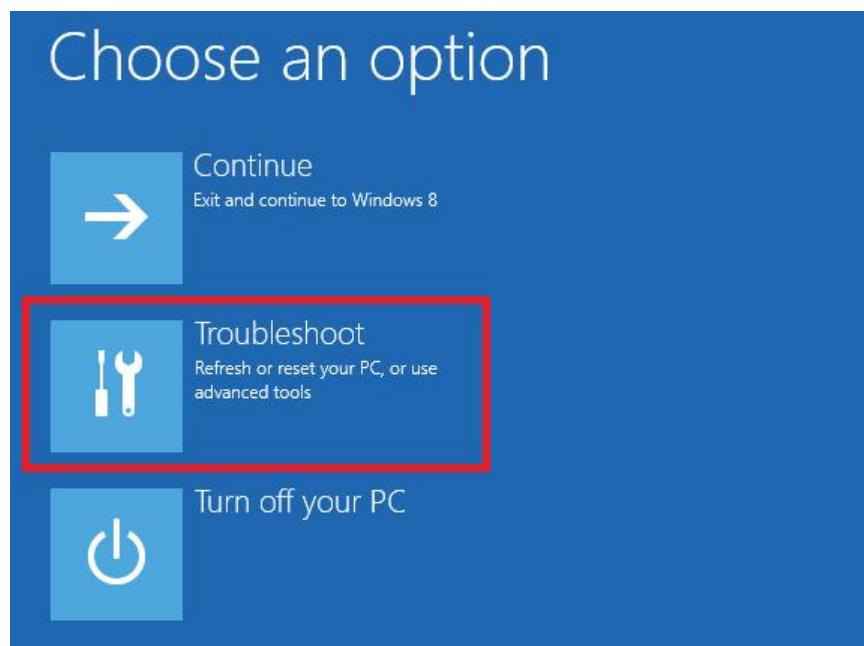
Para iniciar el sistema operativo Windows 8 con la comprobación de la firma digital de los controladores deshabilitada, hay que hacer lo siguiente por pasos.

Pulsar la combinación de teclas **Win+I**, a continuación, manteniendo pulsada la tecla **Shift** seleccionar “Apagar” - “Reiniciar”



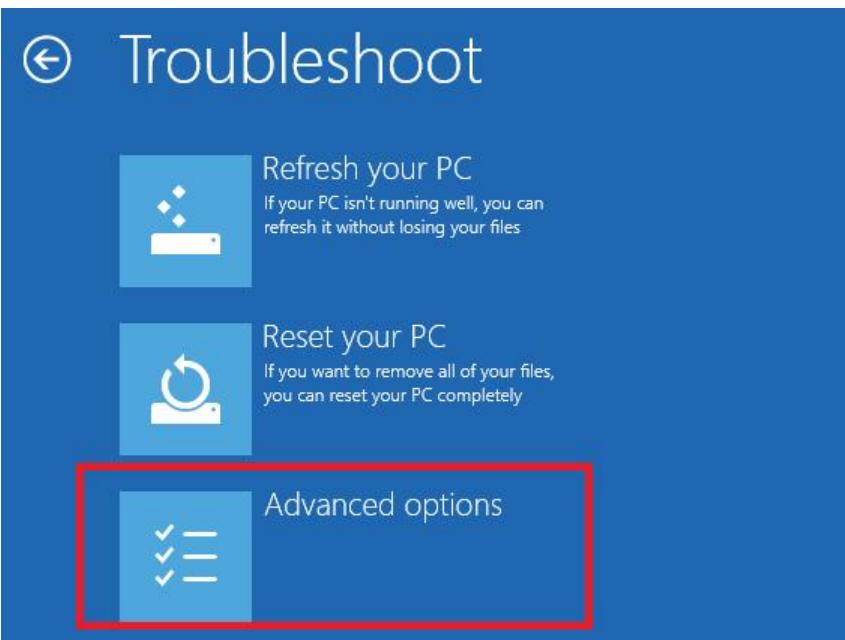
Puc. 38: Reinicio para cambiar los parámetros de inicio

Después de que el sistema operativo se reinicie, aparecerá la ventana de parámetros de inicio. Hay que seleccionar “Solucionar problemas”;



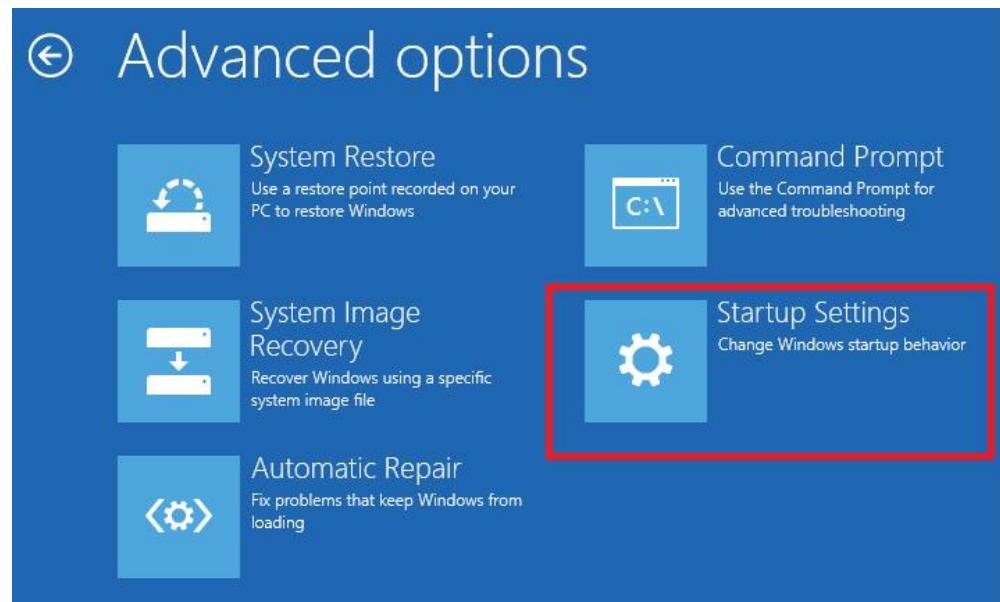
Puc. 39: Entrar en el modo de Solucionar problemas

En la ventana de “Solucionar problemas” hay que seleccionar “Opciones avanzadas”:



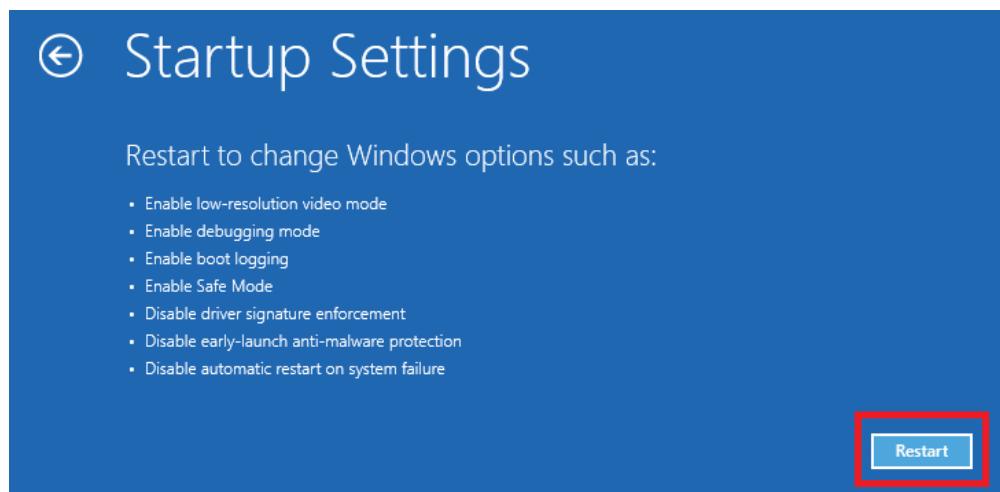
Puc. 40: Opciones avanzadas del menú de Solucionar problemas

En la ventana “Opciones avanzadas” hay que seleccionar “Configuración de inicio”:



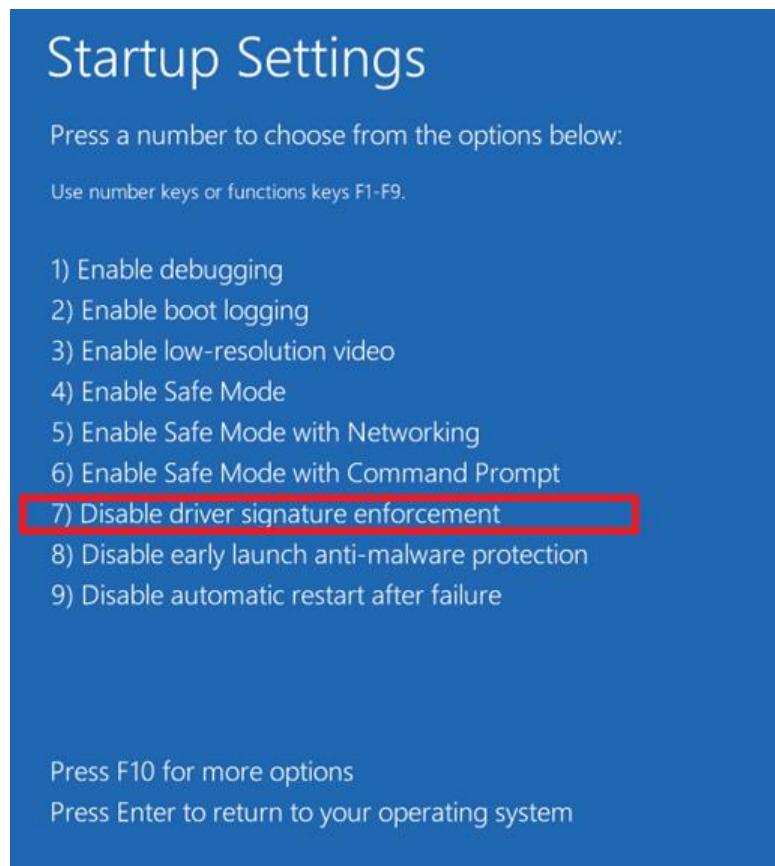
Puc. 41: Configuración de inicio del sistema operativo

En la ventana “Configuración de inicio” hay que pulsar con el botón izquierdo del ratón el botón “Reiniciar”



Puc. 42: Reiniciar

El sistema operativo se reiniciará otra vez y a continuación aparecerá la ventana “**Configuración de inicio**”. En esta ventana hay que pulsar la tecla F7, para continuar el inicio del sistema operativo con la comprobación de la firma digital de los controladores deshabilitada



Puc. 43: Deshabilitar el uso obligatorio de controladores firmados

Después de que el sistema operativo se reinicie, hay que instalar el controlador del equipo de la misma forma que en los sistemas operativos Windows XP / Windows 7. Después de instalar el controlador hay que reiniciar la computadora otra vez para abrir de la comprobación de la firma digital de los controladores.

4.4 Utilidad de actualización del software

El archivo ejecutable de la utilidad se llama **CnordFirmware.exe** y es precisamente el archivo que hay que ejecutar para actualizar la versión del software del equipo.

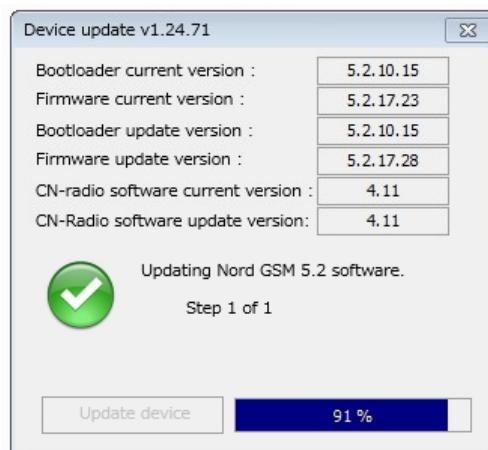
Después de ser iniciada, la utilidad realiza la búsqueda del equipo conectado a la computadora, determina su tipo y muestra la versión del software instalado en el mismo:



Puc. 44: Visualización de la versión del software en el dispositivo

Si la versión del software del dispositivo es inferior a la versión de la actualización, hay que actualizar el firmware en el dispositivo. Para hacerlo hay que pulsar el botón “Actualizar el dispositivo”.

Durante el proceso de la actualización el equipo puede reiniciarse varias veces. Después de que finalice la actualización del firmware del dispositivo, en la ventana de la utilidad aparecerá el correspondiente mensaje:



Puc. 45: Proceso de actualización de la versión del software



Puc. 46: La actualización de la versión del software ha finalizado

A continuación la utilidad para la actualización del firmware por USB se puede cerrar.

Si durante el proceso de la actualización aparece un mensaje de error, se recomienda desconectar el equipo de la computadora, finalizar el trabajo de la utilidad para la actualización de la versión y a continuación conectar de nuevo el equipo a la computadora e iniciar la utilidad.

5 Configuración del dispositivo

Para realizar la configuración (modificar la configuración) del equipo hay un configurador especial, denominado “Hubble”.

La versión actual del configurador se puede descargar desde el sitio oficial del soporte técnico de NTKF “C.Nord” (support.cnord.ru), desde la página “Archivos para descargar”.

El configurador se suministra en forma de archivo zip con el nombre **hubble-X.XX.zip**, donde **X.XX** son los números que corresponden a la versión del configurador. El contenido del archivo hay que descomprimirlo en una carpeta en el disco duro de la computadora y es aconsejable que se haga en una carpeta raíz.

Si por algún motivo no se consigue descomprimir el archivo en la raíz del disco, hay que descomprimirlo en una carpeta cuyo nombre no tenga caracteres cirílicos y espacios. Si esta condición no se cumple, el configurador del equipo funcionará de forma incorrecta.

El archivo ejecutable del configurador se llama **hubble.exe**, precisamente este archivo es el que hay que ejecutar para modificar la configuración del equipo.

El configurador “Hubble” sirve para modificar las configuraciones de los siguientes equipo: “Nord GSM”, “Nord RF”, “Nord LAN”, “Soyuz GSM”, “Soyuz PCB GSM”, “TR-100 GSM IV” y “Serzhant GSM”.

Para empezar a configurar el equipo hay que conectarlo a la computadora por USB e iniciar el configurador. Para iniciar cómodamente el configurador recomendamos ubicar un acceso directo para su inicio en el escritorio o en la carpeta de programas de uso frecuente.

Después de ser iniciado, el configurador detectará automáticamente el equipo conectado a la computadora, realizará la comprobación de la versión del software instalado en el equipo y cargará las configuraciones del equipo.

Si la versión del software instalado en el equipo no corresponde con la versión necesaria para el funcionamiento del configurador, se mostrarán un mensaje de error con la petición de actualizar el software en el equipo. En este caso hay que finalizar el trabajo del configurador y realizar la actualización del software en el equipo, tal como se describe en el apartado “[Actualización del software](#)”.

5.1 Panel de control y panel de pestañas

5.1.1 Panel de control

En la parte superior de la ventana principal del configurador se ubica el panel de control:



Puc. 47: Panel de control

En la parte izquierda del panel de control se muestra la siguiente información:

- tipo de equipo;
- versión del software del equipo;
- versión del software del expansor inalámbrico, si está conectado;
- numero del objeto indicado en la configuración del equipo;
- número de serie del equipo.

El número de serie del equipo se le asigna al ser fabricado y es único para toda la familia de equipos fabricados por la compañía “C.Nord”.

El botón “Leer” sirve para cargar en la interfaz del configurador los ajustes que actualmente están guardados en el equipo. Hay que recordar que si se realiza algún cambio de la configuración del equipo en el configurador, después de pulsar el botón “Leer”, todos los cambios se perderán: las configuraciones realizadas en el configurador serán reemplazadas por las configuraciones cargadas del equipo.

El botón “Grabar” sirve para guardar los cambios de las configuraciones realizadas en el configurador, en el equipo.

El botón “Guardar...” Sirve para guardar en el archivo las configuraciones actuales que se muestran en el configurador. Mediante el botón “Abrir...”, por su parte, se puede cargar la configuración del archivo.

Para evitar errores, relacionados con la configuración de los canales de comunicación, se recomienda guardar en el archivo en el disco todas las configuraciones, relacionadas con la conexión al “Security Center” y a la “Nube”, y en la configuración del equipo que se instala en el objeto, empezar por cargar en el configurador el archivo con estas configuraciones.

5.1.2 Panel de pestañas

En la parte izquierda de la ventana principal del configurador se ubica el panel de pestañas, mediante el cual se realiza el cambio entre los grupos de configuraciones del dispositivo.

Zonas

En la pestaña “Zonas” se realiza la configuración de los parámetros de las zonas por cable conectadas al equipo.

Usuarios

La pestaña «Dispositivos inalámbricos» sirve para conectar al equipo dispositivos - notificadores inalámbricos, llaveros, teclados y retransmisores. Esta pestaña se muestra en el configurador sólo si al equipo está conectado un expansor inalámbrico.

Particiones

Los códigos de usuarios que armarán y desarmarán el sistema de seguridad del equipo se pueden establecer en la pestaña «Usuarios». Aquí también se pueden asignar al usuario una o varias llaves TM, así como especificar el llavero inalámbrico entregado al usuario.

Security center

En la pestaña “Particiones” se puede realizar la configuración de las particiones del objeto. En esta pestaña se pueden especificar las zonas por cable y zonas inalámbricas conectadas a determinadas particiones, así como especificar los usuarios que pueden armar o desarmar el sistema de seguridad de las particiones.

Nube

En la pestaña “Varios” se pueden configurar los intervalos que se usan en la repetición de eventos transmitidos al “Security Center”, especificar el tipo de la fuente de alimentación de reserva conectada al equipo, activar o desactivar el avisador acústico y óptico, etc.

Ethernet

Las configuraciones que debe usar el equipo al transferir eventos por los canales de comunicación GSM y Ethernet se pueden establecer en la pestaña “Security Center”.

Sistemas automáticos

Los parámetros que determinan la transmisión de eventos por el canal de radio, se indican en la pestaña “Radio”.

Historial de eventos

La pestaña “Nube” sirve para especificar a qué “Nube” debe conectarse el equipo para que el técnico tenga la posibilidad de acceder de forma remota al mismo. Los valores de los parámetros en esta pestaña hay que modificarlos sólo si se usa una “Nube privada”, los parámetros para la conexión a la “Nube” deben especificarse de forma manual.

Panel de estado

En la pestaña “Ethernet” se puede cambiar la configuración de la conexión del equipo a la red local. Esta pestaña se refleja en el configurador sólo si al dispositivo está conectado el módulo opcional “Adaptador Ethernet”.

Alarma de incendio

Los parámetros de los operadores de comunicación móvil, tales como la dirección del punto de acceso (APN), el nombre del usuario y la contraseña para el acceso a los servicios de transmisión de paquetes de datos, se pueden modificar en la pestaña “Operadores GSM”.

La pestaña “Sistema automático” sirve para programar el comportamiento del dispositivo dependiendo de unas u otras condiciones. En calidad de condiciones pueden actuar cualesquier eventos creados por el equipo o el tiempo. Y en calidad de acciones que el equipo puede realizar, actúan los armes o desarmes, así como las acciones con los colectores abiertos.

Los eventos que se almacenan en la memoria no volátil del equipo se pueden ver en la pestaña “Historial de eventos”. Aquí también se pueden marcar como enviados los acontecimientos que están a la espera de ser entregados al “Security Center” en la cola de transmisión.

La pestaña “Panel de estado” muestra en tiempo real el estado de los canales de comunicación de las zonas por cable y zonas inalámbricas.

5.2 Zonas

En la pestaña “Zonas” se realiza la configuración de los parámetros de las zonas por cable, conectadas al equipo.

Expansor EW-8 conectado						
Número	Tipo	Norma	Resistencias	Retraso de entrada	Retraso de salida	
1	Activar	De seguridad	Abierto	no hay	15 segundos	15 segundos
2	Activar	De seguridad	Abierto	no hay	sin	sin
3	Activar	De incendio	Abierto	dos		
		De cuatro cables				
4	Activar	Botón de pánico con fijación	Abierto	no hay		
5	Activar	Botón de pánico sin fijación	Abierto	no hay		
6	Activar	24 horas	Abierto	no hay		
7	Activar	24 horas de seguridad	Abierto	no hay		
8	Activar	Fuga de agua	Abierto	no hay		

Puc. 49: Вкладка «Шлейфы»

5.2.1 Expansores

Si el uso de equipos adicionales al equipo “Nord GSM” se pueden conectar hasta 8 zonas por cable. Si se usa el expansor de zonas por cable “EW-8” o “EW-12”, la cantidad de zonas por cable aumenta hasta 16.

“EW-8”

Si al equipo está conectado el expansor “EW-8” hay que marcar la casilla para el parámetro “EW-8” conectado entonces el mecanismo de solicitud de zonas por cable cambia y la cantidad total de zonas en las pestañas aumenta hasta 16.

El esquema de conexión del expansor al equipo, así como los esquemas de conexión de las zonas al expansor, se muestran en el apartado [Conexión del expansor “EW-8”](#).

“EW-12”

Si al equipo está conectado el expansor “EW-12”, en el configurador aparecerán nuevas zonas de forma automática. Los aspectos particulares del funcionamiento y el esquema de conexión del expansor al equipo se muestran en el apartado [Conexión del expansor “EW-12”](#).

El “EW-12” no se puede conectar conjuntamente con el “EW-8”.

5.2.2 Numeración de zonas

Los números de las zonas que se muestran en el configurador corresponden al marcaje de los bornes en la placa de circuito impreso: «Z1» – zona No.1, «Z2» – zona No.2 y sucesivamente.

Si al equipo está conectado el expansor “EW-12”, las zonas del expansor corresponden a los números - 9-16, es decir el borne «Z1» en el expansor corresponde a la zona No.9 en el configurador, el borne «Z2» - a la zona No.10, (. .), el borne «ZN» corresponde a la zona (N+8).

Si al equipo está conectado el expansor “EW-8”, el borne «Z1» sirve para la conexión de dos cables de señal de las zonas No.1 y No.9, el borne «Z2» - para los cables de las zonas No.1 y No.10 y sucesivamente. En otras palabras, el borne «N» sirve para la conexión de cables de las zonas “N” y “N+8”.

5.2.3 Activación y desactivación de la zona

El botón de activación / desactivación de la zona se encuentra en la columna izquierda, directamente detrás del número de la zona. El color del botón refleja el estado actual de la zona: si el botón está verde, la zona está activada, si el botón está rojo, la zona está desactivada. La inscripción en el botón corresponde con la operación que será realizada al pulsar el botón: en el botón verde está escrito “Desactivar”, porque al pulsar el botón la zona será desactivada y en el botón rojo está escrito “Activar”, ya que al pulsar el botón rojo la zona será activada.

Para que el equipo empiece a controlar el estado de la zona y también para que se pueda realizar la configuración de la zona, hay que activarla. Si en el equipo existe aunque sea una zona activada con el tipo “De seguridad”, “De seguridad sin sirena” o “De paso”, tal zona debe ser añadida a la partición.

Si la zona por cable está desactivada, su estado, así como los cambios del estado se ignoran por el equipo. Aparte de esto, si la zona está desactivada, no se puede añadir a la partición: no se reflejará en la lista de zonas disponibles para añadir a la partición..

La desactivación de la zona puede ser útil si temporalmente hay que suspender el control de la zona, por ejemplo, a causa de su mal funcionamiento. La zona se puede desactivar al conectar al equipo de forma local (por USB) y también al conectar de forma remota desde el configurador web.

5.2.4 Tipo de zona

La fijación del tipo de zona es el momento clave en la configuración de la zona, ya que este parámetro determina por completo la reacción del equipo hacia los cambios del estado de la zona. Del tipo que se indica para la zona, depende lo siguiente:

- si el equipo reaccionará sobre el cambio de la zona al estado “Alarma” siempre, o sólo en el momento cuando la partición, a la cual está conectada la zona está armada;
- el código del evento que será transmitido a la consola de seguridad al producirse una alarma en la zona;
- si será activada la sirena al producirse una alarma en la zona;
- si será desactivada y posteriormente activada la alimentación en el borne «SMOKE» al producirse una alarma en la zona;
- si se controlará el estado normal de la zona al armar el sistema de seguridad de la partición, en la cual está conectada.

Las diferencias entre los tipos de zonas por cable se muestran en la tabla más abajo:

Tipo de zona	Códigos de eventos	Arme/desarme	Sirena	Observación
De seguridad	E130 / R130	Si	Si	
De seguridad sin sirena	E146 / R146	Si	No	
De paso	E130 / R130	Si	Si	La alarma en la zona se procesa de una forma especial durante el arme y el desarme (ver más abajo).
De incendio	E110 / R110	No	Si	La alarma en la zona va acompañada por un reseteo de la alimentación de los sensores de incendio (ver más abajo).
Botón de emergencia con fijación	E120 / R120	No	No	
Botón de emergencia sin fijación	E120 / R120	No	No	Para la zona de este tipo se usa un intervalo separado de repetición de alarmas (ver más abajo).
Tamper de sensores	E144 / R144	No	Si	
24 horas de seguridad	E133 / R133	No	Si	
24 horas	E150 / R150	No	Si	
Fuga de agua	E154 / R154	No	Si	
Fuga de gas	E151 / R151	No	Si	
Sensor de temperatura	E158 / R158	No	Si	Alta temperatura
Sensor de temperatura	E159 / R159	No	Si	Baja temperatura

Tipos de zonas por cable

Si para el tipo de zona se indica "Si" en la columna "Arme / desarme", significa que la zona de tal tipo puede ser armada o desarmada junto con cualquier partición a la cual está conectada. Si para el tipo de zona se indica "No" en la columna "Arme / desarme", esto significa que la zona de tal tipo está armada *siempre*.

Si para el tipo de zona se indica "Si" en la columna "Sirena", esto significa que al producirse una alarma en la zona de tal tipo será activada la sirena.

Tipo de zona "De paso"

Si para la zona está indicado el tipo "De paso", tal zona se procesa de una forma especial durante el arme y el desarme.

Al armar el sistema de seguridad el estado de la zona de paso se ignora: el sistema de seguridad del equipo será armado incluso si la zona configurada como de paso está en situación de alarma. Aparte de esto, el estado de la zona de paso se ignora hasta el mismo instante de finalización del retraso de salida para todas las zonas de la partición en la cual se arma el sistema de seguridad. Con ello, el retraso de salida para la misma zona de paso no se puede establecer, esta zona siempre tiene un retraso de salida igual al mayor retraso de salida de otras zonas incluidas en la partición.

Si la partición en la cual está incluida la zona de paso está armada y la zona de paso pasa a situación de alarma,

primero se realiza la verificación del inicio de la cuenta de retraso de salida para otra zona de la partición. Si se está realizando la cuenta de retraso de salida, la alarma en la zona de paso se ignora. Si no hay retraso de salida, en la zona de paso se creará el evento “Alarma” (**E130**).

Tipo de zona “De incendio”

Al formarse la alarma en las zonas con el tipo “De incendio” el equipo aplica el mecanismo “Atención” / “Incendio”: mecanismo basado en la lógica de acción reiterada del avisador después del reseteo de la alimentación. El equipo pasa al estado generalizado “Incendio” que va acompañado con la activación de la sirena de incendio, así como con la repetición de alarmas de incendio. Este estado se guarda en la memoria del equipo, es decir, en caso de reseteo de la alimentación o reinicio del sistema del panel, el estado generalizado “Incendio” se mantiene.

Tipo de zona “Botón de emergencia sin fijación”

Si para la zona se indica el tipo “Botón de emergencia sin fijación”, tal zona tiene un intervalo propio de repetición de alarmas.

Para este tipo de zona el intervalo de repetición de alarmas indicado para el equipo no se usa. En vez de éste se establece un valor equivalente a 5 segundos. De esta forma, la reiterada pulsación del botón de emergencia no antes de 5 segundos generará la transmisión de un evento más a la consola.

Tipo de zona “Sensor de temperatura”

Si al equipo está conectado un sensor de temperatura por cable y el modo de solicitud de la línea 1-Wire está activado (se activa en la pestaña [Varios](#)), éste aparece en la pestaña “Zonas” de forma automática y tendrá un número de zona en el diapasón de 48 a 51. Para los sensores de temperatura debe especificarse el límite superior e inferior, al alcanzar los cuales se formarán las alarmas. Diapasón de valores permitidos para los en límites: de 55 °C bajo cero a 127 °C sobre cero. Más información [sobre la conexión de sensores de temperatura](#). En total al equipo se pueden conectar 4 sensores de temperatura.

5.2.5 Estado normal de la zona

Mediante el valor que se establece en la columna “Norma”, se puede determinar el estado *normal* para la zona de alarma:

- si el estado normal para la zona está determinado como *cerrado*, en tal zona deben usarse avisadores que también disponen de contactos cerrados de su relé de salida en estado normal. En caso de alarma tales avisadores deben *abrir* los contactos del relé de salida;
- si el estado normal para la zona está determinado como *abierto*, en tal zona deben usarse avisadores que disponen de contactos *abiertos* de su relé de salida en estado normal. En caso de alarma tales avisadores deben *cerrar* los contactos del relé de salida.

Hay que destacar que la gran mayoría de los avisadores infrarrojos y de contacto magnético modernos disponen de contactos normalmente cerrados de su relé de salida. De esta forma, para las zonas en las cuales se incluyen estos avisadores, el estado normal debe determinarse como *cerrado*.

5.2.6 Resistencias terminales

Mediante el valor que se establece en la columna “Resistencias” se puede indicar la cantidad de resistencias terminales instaladas en la zona.

Si al conectar la zona no se usan resistencias terminales, para tal zona el equipo puede determinar sólo uno de dos estados: “Alarma” o “Norma”. Tal zona es muy vulnerable: si el estado normal para la zona se determina como *abierto*, es suficiente simplemente con cortar el cable de la zona en cualquier lugar accesible y la zona para siempre se quedará en estado normal, en tal zona nunca se producirá una alarma. Nada mejor será una zona cuyo estado normal está determinado como *cerrado*: si se consigue cerrar los cables de alarma de la zona en cortocircuito, en esta zona tampoco nunca habrá una señal de alarma.

Una resistencia terminal instalada en la zona permite diferenciar un fallo en la zona de una alarma. Qué tipo de fallo puede ser determinado - ruptura o cortocircuito - depende del estado normal de la zona: para el estado normal de la zona *abierto* una resistencia terminal permite determinar la ruptura de la zona y para el estado normal *cerrado* - cortocircuito.

Dos resistencias terminales permiten determinar la ruptura y el cortocircuito para la zona con cualquier estado normal.

Para *minimizar* los fallos de las zonas de alarma, se recomienda conectar a las zonas una resistencia terminal.

5.2.7 Retraso de entrada

El parámetro “Retraso de salida” permite posponer la creación de la señal “Alarma” por el tiempo indicado en calidad de valor para este parámetro. Como norma, este parámetro se establece para las zonas que el usuario debe alterar para llegar al dispositivo de control de la alarma. En calidad de ejemplos extendidos de tales zonas pueden servir los sensores de contacto magnético que protegen las puertas de entrada en los locales bajo alarma.

¿Cómo funciona el retraso de salida? Vamos a suponer que tenemos una zona, en la zona está conectado un avisador de contacto magnético instalado en la puerta de entrada a la oficina. Para esta zona fue establecido un retraso de salida igual a 15 segundos. El panel para teclear el código, con el que se puede desconectar la alarma de seguridad se encuentra dentro de la oficina, es decir hay que abrir la puerta de entrada para llegar al panel. El usuario abre la puerta de entrada, el avisador de contacto magnético se activa, pero el equipo no crea una alarma y empieza la cuenta del retraso de entrada. Si en el transcurso de 15 segundos el usuario introduce el código mediante el cual el sistema de seguridad será desactivado, no se creará una alarma, en vez de la alarma a la consola de seguridad se enviará un evento de desarme del sistema de seguridad del equipo. Si en el transcurso de 15 segundos no se desarma el sistema de seguridad del equipo, se creará una alarma.

El valor del parámetro “Retraso de entrada” se puede especificar sólo para las zonas cuyo tipo está establecido como “De seguridad” o “De seguridad sin sirena”. Esto se debe a que las zonas de todos los demás tipos (excepto la “De paso”) no pueden ser armadas o desarmadas: el sistema de seguridad de esta zona siempre está activado. Lo que respecta al tipo de zona “De paso”, las zonas de este tipo se procesan durante el arme o desarme de una forma especial, según lo descrito más arriba en el apartado “Tipos de zonas”.

Evento “Alarma probable”

Al alterar la zona con retraso de entrada el equipo de forma incondicional crea el evento “Alarma probable” (**E138**). En calidad de argumentos del evento se transmite el número de la zona alterada y el número menor de la partición a la cual está conectada esta zona. Si se alteran varias zonas con retraso de entrada, para cada zona se creará el evento “Alarma probable”.

En algunos objetos el panel de control no se puede ubicar de una forma que se encuentre separada en una parte protegida del local. Normalmente a tales objetos se pueden atribuir pequeños locales: pabellones comerciales, garajes, pequeñas oficinas y apartamentos. Esto significa que durante la cuenta del retraso de entrada el panel de control puede ser estropeado. El evento “Alarma probable” le permite a la consola de seguridad controlar el funcionamiento del equipo después de que empiece la cuenta de retraso de entrada: si después de empezar el retraso de entrada no se recibe el evento sobre el desarme del sistema de seguridad del equipo, es un motivo para informarse de lo que pasa en el objeto.

Para el control automático de recepción del desarme después de una posible alarma en el “Security Center”, hay que usar el procesador de eventos “Entrada a través de la alarma” o el procesador de eventos “Control de la cadena de eventos”.

5.2.8 Retraso de salida

La asignación del parámetro “Retraso de salida” es muy similar a la asignación del parámetro “Retraso de entrada”, pero sirve para darle al usuario la posibilidad de salir del local protegido después de armar el sistema de seguridad del equipo. El retraso de salida, normalmente se establece para las zonas que protegen las puertas de entrada en los locales protegidos.

Después de que el usuario realiza el arme de la partición (mediante el teclado, llavero inalámbrico o lector TM), el equipo comprueba el estado de todas las zonas, incluidas en la partición:

- si se detecta una zona que no funciona, el equipo deniega el arme;
- si se detecta una zona bajo alarma, el equipo también deniega el arme;
- si no hay zonas que nos funcionan o zonas bajo alarma, el equipo se arma y empieza la cuenta de retraso de salida, si tiene lugar.

El evento sobre el arme (**E401**) se crea directamente al realizar el arme, antes del inicio del retraso de salida, si tiene lugar. En calidad de argumentos del evento se transmite el número de la partición armada, así como el numero del usuario que realizó el arme.

Después de que haya empezado el retraso de salida, el equipo ignora el estado de todas las zonas para las cuales está establecido el retraso de salida, así como de las zonas con tipo “De paso”. Si al usuario le da tiempo salir del local y cerrar la puerta de entrada antes de que finalice la cuenta de retraso de salida, no se producirá una alarma después del arme. Si alguna de las zonas será alterada después de que finalice el retraso de salida, se creará una alarma.

Para los dispositivos inalámbricos por actual se toma el estado que fue recibido durante la última solicitud del dispositivo. De esta forma, el usuario del sistema inalámbrico podrá tener que esperar mientras el avisador inalámbrico no devuelva el equipo a la norma. En el caso de que no se desee esperar, para los avisadores inalámbricos se puede establecer el mínimo retraso posible de salida.

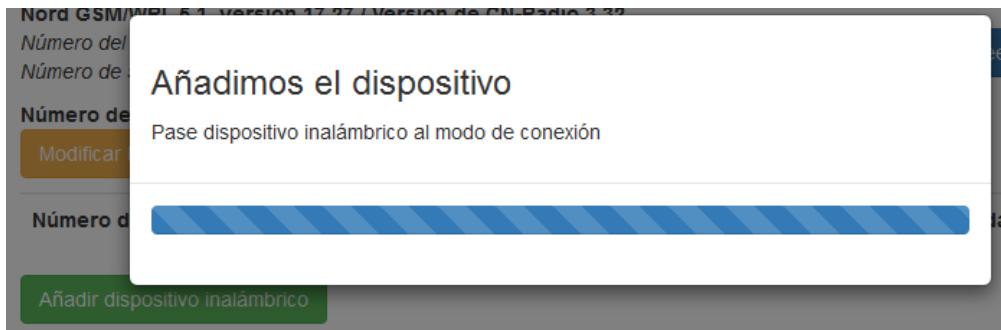
Puede darse la situación que durante el arme no se pueda alcanzar el estado normal de una o varias zonas, por ejemplo si los avisadores en las zonas controlan una parte del teclado. En este caso las zonas hay que configurarlas como *de paso*. Las zonas de paso se describen más arriba con mayor detalle, en el apartado “*Tipos de zonas*”.

La alarma en las zonas con retraso de salida para el momento del arme se ignora. Esto se hace para que el usuario no tenga que comprobar y cerrar la puerta de entrada. Pero si desea tener la seguridad de que todas las zonas de alarma están bajo la norma para el momento del arme, se puede activar el control de alarma en las zonas con retraso de salida para el momento del arme. Para ello hay que marcar la casilla para los parámetros “Prohibir el arme en caso de alarma en la zona con retraso de salida”, que se encuentra en el apartado “*Varios*”, en el apartado “*Arme y desarme*”.

5.3 Dispositivos inalámbricos

Mediante la pestaña «Dispositivos inalámbricos» en el equipo se graban los dispositivos inalámbricos y sus parámetros, tales como el tipo, el retraso de entrada, retraso de salida, etc. Todos los dispositivos inalámbricos se conectan al equipo “Nord GSM” a través del expansor “SN-Radio”. El expansor soporta la conexión de 31 dispositivo. Toda la lista de dispositivos se encuentra en el [sitio](#).

5.3.1 Conexión del dispositivo al equipo



Puc. 50: Adición de dispositivo, Pestaña «Dispositivos inalámbricos»

La mayoría de dispositivos

Para conectar los dispositivos CN-PIR, CN-PIR-Outdoor, CN-PIR-Mini, CN-Magnetic, CN-Magnetic-Mini, CN-Glass, CN-Fire, CN-Flood, CN-Flood-Mini, CN-Celsius, CN-Keypad, CN-Repeater, CN-Repeater 220, CN-Exit, CN-Smoke hay que hacer lo siguiente:

- Quitar la tapa del dispositivo;
- Instalar los elementos de alimentación;
- En la pestaña «Dispositivos inalámbricos» del configurador pulsar el botón *Añadir dispositivo inalámbrico*;
- Cambiar el dispositivo inalámbrico al modo de unión mediante el cierre momentáneo de los contactos “Reseteo”.

Con destellos del LED verde el dispositivo confirmará el paso al modo de unión La activación del indicador rojo por 2 segundos avisa que la conexión del dispositivo al equipo se ha realizado con éxito

CN-Siren

Para conectar los dispositivos de tipo “CN-Siren” y “CN-Smoke” hay que hacer lo siguiente:

- Quitar la tapa delantera, instalar los elementos de alimentación;
- En la pestaña «Dispositivos inalámbricos» del configurador, pulsar el botón *Añadir dispositivo inalámbrico*;
- Cambiar el dispositivo inalámbrico al modo de unión, cerrando el contacto “negativo” del fijador de la batería y el contacto “4” en la base del avisador.

La activación del indicador rojo por 2 segundos avisa que la unión se ha realizado con éxito.

CN-KeyFob

Para conectar el dispositivo CN-KeyFob al equipo hay que hacer lo siguiente:

- Abrir el cuerpo del llavero, instalar la batería en el fijador, cerrar el cuerpo;
- En la pestaña «Dispositivos inalámbricos» del configurador, pulsar el botón *Añadir dispositivo inalámbrico*;
- Pulsar y soltar cualquier botón en el llavero. El dispositivo periódicamente activará el indicador de color verde, lo que evidencia que se encuentra en el modo de “Unión”. Si la indicación especificada no tiene lugar, pulsar y mantener pulsados al mismo tiempo los tres botones durante 2 segundos y más, con ello el indicador debe activarse en color verde. Mantener los botones hasta que se active el indicador en color rojo.

Si el llavero servirá en calidad de Botón de emergencia, después de la unión hay que marcar la casilla “Botón de emergencia activado”.

5.3.2 Retransmisor

“CN-Repeater” y “CN-Repeater 220” son retransmisores que sirven para aumentar la distancia de funcionamiento de los dispositivos inalámbricos.

Después de que aunque sea un retransmisor sea conectado al equipo en la pestaña «Dispositivos inalámbricos» en la columna “A través del retransmisor” para cada dispositivo aparecerá la posibilidad de elegir cómo este dispositivo debe transmitir las señales al equipo: directamente o a través del retransmisor especificado.

Número de la zona	Sensor	Tipo / Modo	Retraso de entrada	Retraso de salida	A través del transmisor		
17		Repeater	24 horas				
18		PIR	De seguridad	30 segundos	1 minuto	17	
19		PIR	De paso			17	
20		KeyFob	<input checked="" type="checkbox"/> Botón de pánico activado		sin		

Puc. 51: Dispositivos inalámbricos configurados para funcionar a través del retransmisor

Preste atención que la conexión (unión) de cualquier dispositivo siempre se realiza directamente al equipo. Después de que se realice la conexión, el dispositivo se puede cambiar al modo de transmisión de señales a través del retransmisor.

No se puede crear una cadena de retransmisores: entre el equipo y el dispositivo inalámbrico sólo puede haber un retransmisor.

El algoritmo de funcionamiento de dispositivos inalámbricos está realizado de tal forma que si el retransmisor se estropea y el equipo “oirá” el dispositivo sin el retransmisor, la recepción de señales de tales dispositivos se realizará sin el retransmisor.

5.3.3 Recomendaciones de montaje

1. La instalación del panel hay que realizarla en un lugar que se encuentre en acceso directo por radio hacia los lugares previstos de la instalación de avisadores, donde no haya construcciones metálicas y otras construcciones que puedan apantallar. Por ejemplo, detrás de la pared del lugar de la instalación del panel puede haber una caja de ventilación que obstaculiza el paso de la señal;
2. Para mejorar un poco los parámetros de la vía de radio se puede enderezar la antena del expansor CN-Radio y sacarla fuera de los límites del cuerpo del panel;
3. La comprobación de los lugares de la instalación de los sensores de radio debe realizarse en la posición de las puertas/ventanas/portales/rejas actual para el momento del arme del sistema de seguridad - normalmente, en estado cerrado;
4. En el supuesto lugar de instalación del sensor no debe haber construcciones metálicas en la base de la pared (perfil metálico/armadura);
5. Al elegir el lugar de la instalación, hay que determinar la calidad de comunicación entre el dispositivo y el equipo.

Para comprobar la calidad de comunicación en la parte del dispositivo inalámbrico hay que pulsar y mantener pulsado durante 3 segundos el tamper del dispositivo. Si el LED verde parpadea más de una vez, la calidad de la conexión es buena. Si se enciende el LED rojo, hay que cambiar el lugar de instalación del dispositivo.

Para comprobar la calidad de comunicación en la parte del equipo hay que guardar la configuración en el equipo y después abrir la pestaña “Panel de estado” - «Dispositivos inalámbricos». Si para el dispositivo seleccionado el valor de la calidad de conexión está marcado como “malo”, se recomienda cambiar el lugar de la instalación prevista del dispositivo o usar el retransmisor “CN-Repeater”.

5.4 Usuarios

En la pestaña “Usuarios” se realiza la creación de los usuarios del objeto. En el equipo se pueden crear hasta 32 usuarios y cada usuario aparte de su código personal, también puede tener llaveros inalámbricos y llaves TM.

Número	Código	Claves	Llaveros
1	<input type="button" value="Modificar"/>	+	<input type="button" value="Borrar"/>
2	<input type="button" value="Modificar"/>	+	<input type="button" value="Borrar"/>
3	<input type="button" value="Modificar"/>	+	<input type="button" value="Borrar"/> × Llavero №1

Puc. 52: Pestaña «Usuarios»

Para crear un nuevo usuario hay que pulsar el botón *Añadir usuario* y en la ventana abierta introducir el código que usará el usuario creado al armar el sistema de seguridad del objeto y desarmarlo.

Nuevo usuario

El código debe componerse de 4 números, ser único y ser diferente del código de desactivación de la sirena (5422).

Puc. 53: Pestaña «Usuarios», diálogo de introducción del código

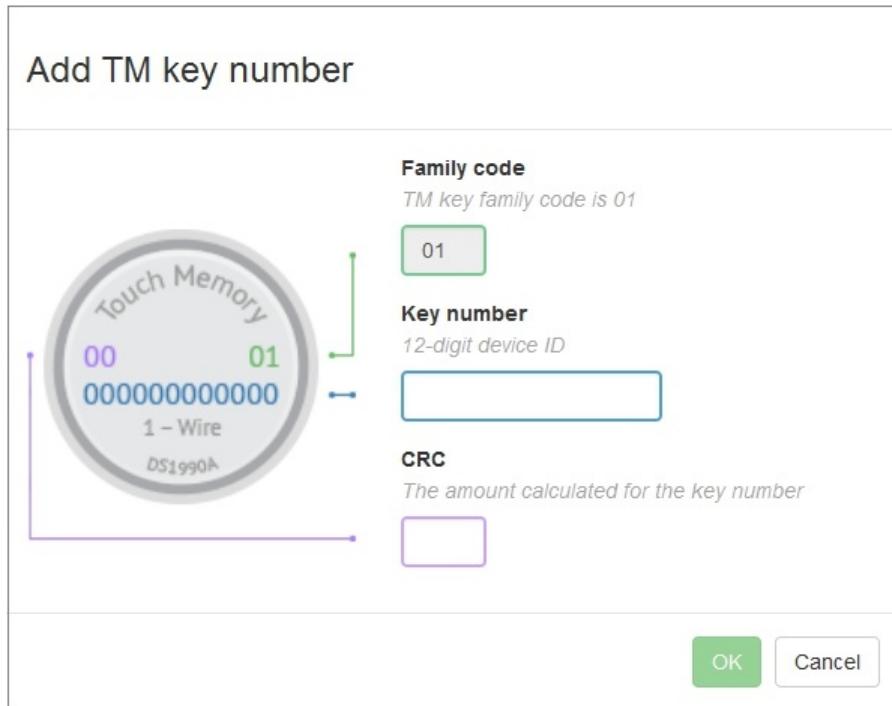
Para añadir una llave Touch Memory enfrente del usuario seleccionado hay que pulsar el botón **Leer** en la columna “llaves”, a continuación poner la llave TM en el lector. Si el lector está conectado correctamente, se mostrará el código de la llave. La llave TM se puede añadir al usuario de forma manual. Para hacerlo hay que pulsar el botón **Introducir el numero** y en la ventana que se abra introducir la información de la llave.

A continuación hay que ir a la pestaña **Particiones** y añadir la llave a la partición que se va a controlar con esta llave. A un usuario se pueden añadir varias llaves TM, pero mediante una llave TM sólo se puede controlar el estado de una sola partición.

Añadimos la llave para el usuario №2

Ponga la llave en el lector

Puc. 54: Apartado «Usuarios», adición de la llave TM



Puc. 55: Pestaña «Usuarios», adición del número de la llave TM de forma manual

Si al equipo está vinculado un llavero inalámbrico, se puede añadir a un usuario concreto mediante el botón *Añadir llavero*. El llavero inalámbrico se debe conectar el equipo en la pestaña «[Dispositivos inalámbricos](#)». Después de que el llavero sea añadido, hay que pasar a la pestaña «[Particiones](#)» y asignar el llavero a la partición que éste controlará.

Número	Código	Claves	Llaveros
1	Modificar	+	Añadir llavero
2	Modificar	+	Añadir llavero

[Añadir usuario...](#)

Puc. 56: Pestaña «Usuarios», adición de llavero

Mediante el ícono de la papelera se pueden eliminar usuarios creados anteriormente.

5.5 Particiones

En la pestaña “Particiones” se realiza la configuración de las particiones del objeto. En el dispositivo se pueden crear hasta 32 particiones con la posibilidad de su arme y desarme independiente.

Número	Zonas	Arme y desarme
1	<input checked="" type="checkbox"/> №1, De seguridad <input checked="" type="checkbox"/> №2, De paso Añadir zona ▾	<input checked="" type="checkbox"/> Usuario №1, código Añadir código ▾
2	<input checked="" type="checkbox"/> №3, De seguridad <input checked="" type="checkbox"/> №8, Fuga de agua Añadir zona ▾	<input checked="" type="checkbox"/> Usuario №2, código Añadir código ▾
3	<input checked="" type="checkbox"/> №19, De paso <input checked="" type="checkbox"/> №21, De seguridad Añadir zona ▾	<input checked="" type="checkbox"/> Usuario №3, llavero 1 Añadir código ▾
Añadir partición		

Puc. 57: Pestaña «Particiones»

Para crear una partición hay que pulsar el botón “Añadir partición”. A cada partición se le asigna su número, los números se generan de forma consecutiva de 1 a 32. Para cada partición existe el botón “Añadir zona” y “Añadir código”, ubicadas en la segunda y tercera columna correspondientemente.

Mediante el botón “Añadir zona” en el menú emergente se pueden seleccionar las zonas que serán añadidas a esta partición. En el menú emergente sólo se muestran las zonas *activadas*.

Mediante el icono de la papelera se pueden eliminar las zonas creadas anteriormente.

5.5.1 Control de particiones

Para que el usuario pueda usar su código personal al armar la partición y desarmar la partición, al usuario hay que vincularlo a esta partición. Para hacerlo hay que pulsar el botón “Añadir código” y en la lista emergente seleccionar aquellos usuarios que podrán controlar la partición concreta.

Si el usuario tiene un llavero inalámbrico o una llave TM y con ellos quiere controlar los dispositivos, éstos también deben añadirse a la partición seleccionada.

Es importante tener en cuenta lo siguiente:

- Si la llave TM o el llavero no está añadido a ninguna partición, automáticamente será asignado a la primera partición.
- Con un llavero no se pueden controlar varias particiones, sólo una. La misma situación se da con la llave TM: a una llave sólo puede corresponder una partición.
- A un usuario pueden asignarse varias particiones. Entonces, para armar y desarmar el usuario deberá indicar el número de la partición que desea armar o desarmar.
- Una misma zona puede ser añadida a varias particiones, pero con ello hay que recordar que el sistema de seguridad de la zona está armado, cuando todas las particiones en las que entra la zona están armadas.

5.6 Varios

En la pestaña “Varios” se pueden especificar diferentes parámetros que determinan el funcionamiento del equipo.

5.6.1 Intervalos

Parámetro	Valor
Intervalo de repetición de alarmas	5 minutos
Intervalo de repetición de alarmas de incendio	24 horas
Intervalo de repetición de fallos	15 minutos
Intervalo de cambio al canal principal	5 minutos
Intervalo de transmisión de pruebas	1 hora
Intervalo de control de transmisión de eventos	7 minutos
Intervalo de control de comunicación con dispositivos inalámbricos, con el sistema de alarma desarmado	5 minutos
Intervalo de control de comunicación con dispositivos inalámbricos, con el sistema de alarma armado	5 minutos

Puc. 58: Pestaña «Varios», apartado «Intervalos»

Intervalo de repetición de alarmas

Mediante el parámetro “Intervalo de repetición de alarmas” se puede establecer el intervalo con el cual el dispositivo creará alarmas *similares* y las transmitirá a la consola de seguridad. Se consideran *similares* las alarmas que surgieron en la misma zona por cable y fueron transmitidas por el mismo avisador inalámbrico.

El valor del parámetro “Intervalo de repetición de alarmas” se aplica para las zonas de todos los tipos, a excepción de las zonas con el tipo “De incendio” y “Botón de emergencia sin fijación”. El intervalo de repetición de alarmas para las zonas con el tipo “Botón de emergencia sin fijación” siempre es igual a 5 segundos y el intervalo de repetición de alarmas para las zonas con el tipo “De incendio”, se asigna por un parámetro aparte (ver más abajo).

¿Para qué sirve este parámetro? En primer lugar, para reducir la cantidad de eventos que se transmitirán a la consola de seguridad: un evento de emergencia puede ser completamente suficiente para que el operador empiece a procesar la alarma en el objeto. La alarma reiterada en la misma zona, como norma, no cambiará nada. En el caso de que el dispositivo detecte una alarma en otra zona, tal alarma será transmitida a la consola y para esta zona empezará la cuenta del propio intervalo de repetición de alarmas.

Si para el parámetro “Intervalo de repetición de alarmas” fue establecido cualquier valor numérico, el dispositivo formará eventos por la zona concreta de la siguiente forma:

- al detectar una alarma en la zona se creará un evento de alarma y empezará la cuenta del intervalo establecido;
- al detectar un reseteo de la alarma en la zona se creará un evento de reseteo, la cuenta del intervalo establecido continuará;
- en caso de creación reiterada de una alarma o reseteo de una alarma en la zona los eventos no se crearán hasta que no finalice la cuenta del intervalo establecido.

El valor numérico significa que durante el intervalo sólo será transmitida una alarma y reseteo por una de las zonas.

Si para el parámetro “Intervalo de repetición de alarmas” está establecido el valor “No repetir”, el dispositivo formará los eventos de la siguiente forma:

- al detectar una alarma en la zona se creará un evento de alarma y empezará la espera del reseteo de la alarma en la zona;

- el evento reiterado sobre la alarma en la zona no se creará hasta que en la zona no se forme un evento de reseteo de la alarma;
- al detectar el reseteo de la alarma en la zona, se formara un evento de reseteo, la espera del reseteo de la alarma en la zona finalizará, el equipo creará un evento de alarma en la zona de nuevo, cuando sea detectada.

El valor “No repetir” significa que la alarma reiterada en la zona puede ser transmitida sólo después de que a través de la zona se transmita el reseteo de la alarma anterior.

El parámetro “Intervalo de repetición de alarmas” no se extiende sobre las alarmas que se forman al accionarse el tamper del equipo. Los eventos de alteración o recuperación del tamper siempre se crean basándose en el cambio del estado del tamper.

Intervalo de repetición de alarmas de incendio

El parámetro “Intervalo de repetición de alarmas de incendio” establece el intervalo con el cual el equipo creará alarmas similares por las zonas de tipo “De incendio” y las transmitirá a la consola de seguridad. Se consideran similares las alarmas que surgieron en la misma zona o fueron transmitidas por el mismo avisador inalámbrico.

El intervalo de repetición de alarmas de incendio por una parte sirve para reducir la cantidad de eventos similares que serán transmitidos a la consola de seguridad, y por otra parte - para no permitir la situación bajo la cual el personal de la consola de seguridad perderá de vista el hecho de que el dispositivo en el objeto se encuentra en estado generalizado “Incendio”; si el [reseteo automático del estado generalizado “Incendio”](#) está prohibido, para su reseteo hay que teclear el código en el teclado.

El valor para el parámetro “Intervalo de repetición de alarmas de incendio” se usa de la siguiente forma:

- al detectar una alarma de incendio en la zona, se creará el evento “Incendio”, el dispositivo pasará al estado “Incendio” y empezará la cuenta del intervalo establecido;
- al finalizar la cuenta del intervalo establecido, el evento “Incendio” se creará de forma reiterada en todas las zonas, por las cuales fue creado durante la cuenta del intervalo. Después de esto la cuenta del intervalo empezará de nuevo;
- al resetear el estado generalizado “Incendio” la cuenta del intervalo será finalizada.

Intervalo de repetición de fallos

Mediante el parámetro “Intervalo de repetición de fallos” se puede establecer el intervalo con el cual el dispositivo creará fallos *similares* por zonas y dispositivos inalámbricos conectados al equipo. Se consideran *similares* los fallos que surgieron en la misma zona por cable o fueron transmitidos por el mismo dispositivo inalámbrico. Con ello, a diferencia de los intervalos de repetición de alarmas de seguridad o alarmas de incendio, la cuenta del intervalo de repetición de fallos *finaliza*, si se detecta la recuperación del estado del fallo y se crea el evento correspondiente.

Para las zonas por cable son fallos sobre los cuales se extiende el “Intervalo de repetición de fallos” los fallos físicos de la zona - ruptura y cortocircuito. Estos fallos se crean solo en el caso de que a la zona esté conectada una o dos resistencias terminales.

Si para la zona por cable se indica un tipo que supone el arme del sistema de seguridad, entonces los códigos de los eventos que se crean al detectar fallos/recuperaciones en tal zona, dependerán del estado (armado o desarmado) en el cual estaba la zona para el momento de la detección del fallo:

- los códigos **E331/R331** se crearán al detectar una ruptura/recuperación de la zona *desarmada*;
- los códigos **E141/R141** se crearán al detectar una ruptura/recuperación de la zona *armada*;
- los códigos **E332/R332** se crearán al detectar un cortocircuito/recuperación de la zona *desarmada*;
- los códigos **E142/R142** se crearán al detectar un cortocircuito/recuperación de la zona *armada*;

A pesar de que los códigos **E141** y **E142** se consideran como alarmas, sobre los eventos con estos códigos se extiende el intervalo de repetición de fallos y no alarmas.

La lista de fallos para los dispositivos inalámbricos, sobre los cuales se extiende el “Intervalo de repetición de fallos” es la siguiente:

- pérdida de conexión;
- descarga de la batería principal;
- descarga de la batería de reserva (si la instalación de la batería de reserva se prevé por la construcción del equipo);

- fallo de la zona del sensor de inundación, conectado al avisador “CN-Flood” (individual para cada zona), fallos del sensor de temperatura.

El valor del parámetro “Intervalo de repetición de fallos” no se extiende sobre los siguientes eventos de fallos que se crean por el equipo: * descarga de la batería de reserva, conectada al equipo. El evento sobre la descarga de la batería de reserva (código **E302**) se crea una vez y se repite sólo al activar el equipo; * fallo de la batería de reserva conectada al equipo. El evento de fallo de la batería de reserva (código **E309**) se crea cada 12 horas, según los resultados de cada comprobación de la calidad de la batería de reserva;

Intervalo de cambio al canal principal

Mediante el parámetro “Intervalo de cambio al canal principal” se puede establecer el intervalo dentro del cual el equipo intentará inicializar la conexión a la consola a través del canal IP que es principal. Qué canal de comunicación es principal depende de si al equipo está conectado el “Adaptador Ethernet”:

- si el “Adaptador Ethernet” está conectado al equipo, el canal principal de comunicación es Ethernet;
- si el “Adaptador Ethernet” no está conectado al equipo, el canal principal de comunicaciones es el canal GPRS en la SIM1.

Puede informarse con mayor detalle sobre las particularidades de la configuración de los canales IP, así como de las normas de cambio de canales de comunicación en el apartado de la descripción, dedicado a la [pestaña “Security Center”](#).

Hay que destacar que en calidad de valor para el parámetro “Intervalo de cambio al canal principal” se puede indicar el valor “No cambiar”. En este caso el cambio forzado al canal principal de comunicación será desactivado. Tal posibilidad permite usar tarjetas SIM “equivalentes” - si el equipo se conectó a través de GPRS en la SIM2, permanecerá en este canal hasta que el canal funcione.

Intervalo de transmisión de pruebas

Mediante el parámetro “Intervalo de transmisión de pruebas” se puede establecer el intervalo con el cual el equipo generará un evento de prueba y lo enviará a través del canal de comunicación disponible en aquel momento. Es importante comprender que este intervalo siempre se cuenta del último evento que fue transmitido por el equipo. Si al finalizar el intervalo no se producen eventos para la transmisión, se formará y se transmitirá un evento de prueba. Si para este parámetro se indica el valor “No transmitir”, el equipo no formará el evento de prueba (código **E602**).

Intervalo de control de transmisión de eventos

Mediante el parámetro “Intervalo de control de transmisión de eventos” se establece el intervalo durante el cual el sistema de auditoría espera el envío del evento. El *sistema de auditoría* es un mecanismo de software que controla el hecho de transmisión de eventos a la consola de seguridad.

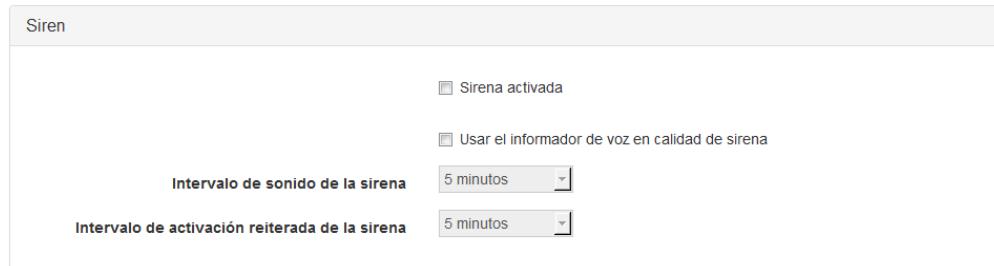
Si para el parámetro “Intervalo de control de transmisión de eventos” se establece cualquier valor numérico, el dispositivo funcionará de la siguiente forma:

- Si el sistema de auditoría registra una ausencia de transmisión de eventos en el intervalo de tiempo indicado en el parámetro, primero se realiza el cambio del canal de comunicación que se usa por el equipo actualmente;
- En el momento cuando el sistema de auditoría realizó el cambio del canal de comunicación se forma el evento con el código E754. Como argumento para el evento con el código E754 sirve el tipo de canal de comunicación que dejó de transmitir eventos (1 - Ethernet o GSM, 3 - radio). El valor del argumento se transmite al campo destinado al número de zona o usuario.
- Si el cambio del canal no ayudó y los eventos siguen sin enviarse, a través del intervalo de control de transmisión de eventos el sistema de auditoría realiza el reinicio del equipo.
- Después del reinicio se formarán dos eventos. Código del primer evento - R305, este evento registra el hecho de reinicio del equipo. El código del segundo evento - R754, este evento significa que el reinicio tuvo lugar por orden del sistema de auditoría.

El valor predeterminado para este parámetro es de 7 minutos. Si hace falta el valor se puede aumentar. Si para este parámetro se establece el valor “No controlar”, el sistema de auditoría será desactivado.

Intervalos de control de comunicación con dispositivos inalámbricos

“El intervalo de control de comunicación con dispositivos inalámbricos” es el intervalo, en el transcurso del cual del dispositivo inalámbrico debe recibirse aunque sea un envío. Si en el transcurso de este intervalo el dispositivo inalámbrico no envía nada, se creará el mensaje de pérdida de conexión. Los dispositivos inalámbricos mandan envíos de prueba una vez cada 30 segundos. Si para este parámetro se indica el valor “No controlar”, el dispositivo no controlará los envíos de prueba de los dispositivos inalámbricos. ### Sirena {#config-misc-siren}



Puc. 59: Pestaña «Varios», apartado «Sirena»

Sirena conectada

Si la sirena está conectada a su correspondiente salida “Sirena”, hay que marcar la correspondiente casilla. Con ello, se activará el control de líneas de conexión con la sirena que permite detectar la ruptura y el cortocircuito de la línea, en caso de sirena desactivada y en caso de sirena activada. Si se detecta cualquiera de los fallos especificados se crea un evento con el código **E321 - Fallo de la sirena**, que se transmite a la consola de seguridad.

Aparte de conectar en la salida de la sirena, la sirena se puede conectar a cualquiera de los siete colectores abiertos, con ello no hay que marcar la casilla “Sirena conectada”. Es importante destacar que el equipo no controla el estado de la línea, si la sirena está conectada a un colector abierto.

La conexión de la sirena a un colector abierto se realiza de la siguiente forma:

- El cable “Positivo” del avisador puede ser conectado a cualquier salida positiva del panel de control, por ejemplo, la salida para la alimentación del teclado o las zonas.
- El cable “Negativo” del avisador debe ser conectado a uno de los siete colectores abiertos: FIRE, DEFECT, LED_G, LED_Y, FIRE2, DEFECT2, DISABL.
- Despues de conectar el avisador, hay que configurar la salida mediante las normas del sistema automático. Puede informarse con mayor detalle sobre las normas en el [apartado Sistema automático](#)

Intervalo de sonido de la sirena

El parámetro “Intervalo de sonido de la sirena” es responsable por la duración del sonido de la sirena, independientemente de la forma de su conexión. Al transcurrir el tiempo indicado en el valor del parámetro, la sirena dejará de sonar.

Intervalo de activación reiterada de la sirena

En el valor del parámetro “Intervalo de activación reiterada de la sirena”, se indica el tiempo, dentro del cual la sirena empezará a sonar de nuevo si no tuvo lugar el reseteo de la alarma.

5.6.2 Alimentación de reserva

Tipo de fuente de alimentación de reserva

En el punto “Tipo de fuente de alimentación de reserva” se puede especificar qué fuente de reserva está conectada al dispositivo: batería o fuente de alimentación ininterrumpida.

Si está conectada la batería

Alimentación de reserva

Tipo de fuente de alimentación de reserva	Batería
<input checked="" type="checkbox"/> Proteger la fuente de reserva contra descarga profunda	
<input checked="" type="checkbox"/> Comprobar la calidad de la batería	

Puc. 60: Pestaña «Varios», apartado «Alimentación de reserva»

Si en calidad de fuente de reserva fue elegida la batería, existe la posibilidad de activar dos parámetros:

- *Proteger la fuente de reserva contra la descarga profunda.*

Si este parámetro está activado, al alcanzar una tensión de 8,5 V en los bornes de la batería, el equipo se desconectará para prevenir la posibilidad de descarga de la batería hasta un nivel crítico, en el cual su carga no puede ser recuperada.

- *Comprobar la calidad de la batería.*

Para comprobar la calidad de la batería el equipo conecta periódicamente la carga y controla la caída de la tensión. Si el valor de la caída de la tensión bajo la carga superó 2 V, se forma el evento **E309 - Fallo de la batería**.

Si está conectada la fuente de alimentación ininterrumpida

Alimentación de reserva

Tipo de fuente de alimentación de reserva	SAI
<input type="checkbox"/> Proteger la fuente de reserva contra descarga profunda	
<input type="checkbox"/> Comprobar la calidad de la batería	

Puc. 61: Pestaña «Varios», apartado «Alimentación de reserva», seleccionado el valor "Fuente de alimentación de reserva" para el parámetro "Tipo de fuente de alimentación de reserva".

Si en calidad de fuente de reserva fue seleccionada la fuente de alimentación de reserva, no se pueden activar los parámetros adicionales (protección contra la descarga profunda y control de la calidad de la batería). ### Arme y desarme

En este apartado se pueden especificar diferentes parámetros que influirán en el proceso de arme del sistema de seguridad y desarme del sistema de seguridad.

Arme y desarme

- Prohibir el arme en caso de alarma en las zonas con retraso de salida
 - Prohibir el arme en caso de que no esté disponible la fuente principal de alimentación (220 V)
- Prohibir el arme al no haber comunicación IP con «Security center»
- Permitir el arme y desarme remoto desde el «Security center»
- Activar códigos de desarme bajo obligación

Se considera código de desarme bajo obligación el código que se diferencia del código del usuario en una unidad en dirección mayor o menor. Por ejemplo, si el código del usuario es «1234», los códigos de desarme bajo obligación serán «1233» y «1235». Teniendo en cuenta:

 - si el código del usuario termina con el número «0», el código de desarme bajo obligación solo será uno – en una unidad superior. Por ejemplo, si el código del usuario es igual a «5840», el código de desarme bajo obligación solo será el código «5841».
 - si el código del usuario termina con el número «9», el código de desarme bajo obligación también será solo uno – en una unidad inferior. Por ejemplo, si el código del usuario es igual a «5849», el código de desarme bajo obligación solo será el código «5848».
- No indicar el retraso de entrada en CN-Keypad

La desactivación de la indicación de retraso de entrada permitirá aumentar el tiempo de funcionamiento de las baterías en el teclado CN-Keypad.

Puc. 62: Pestaña «Varios», apartado «Arme y desarme»

Prohibir el arme en caso de alarma en las zonas con retraso de salida

De forma predeterminada la alarma en las zonas con retraso de salida se ignora para el momento del arme del sistema de seguridad. Esto está hecho para que el usuario pueda armar el sistema de seguridad del objeto y cerrar tranquilamente la puerta de entrada. Pero si desea tener la seguridad de que todas las zonas de alarma están bajo la norma para el momento del arme, se puede activar el control de alarma en las zonas con retraso de salida. Para ello hay que marcar la casilla para los parámetros *Prohibir el arme en caso de alarma en la zona con retraso de salida*.

Prohibir el arme en caso de ausencia de la alimentación principal (220 V)

Al establecer este parámetro, será imposible armar el equipo si el equipo funciona con alimentación de reserva y no hay alimentación principal.

Prohibir el arme en caso de ausencia de comunicación IP con el “Security Center”

Al establecer este parámetro, será imposible armar el equipo si no hay comunicación por GPRS o Ethernet.

Permitir el arme y el desarme remoto desde el “Security Center”

La activación de este parámetro permitirá controlar de forma remota el estado del sistema de seguridad desde la aplicación móvil y la consola de seguridad.

Activar los códigos de desarme forzado

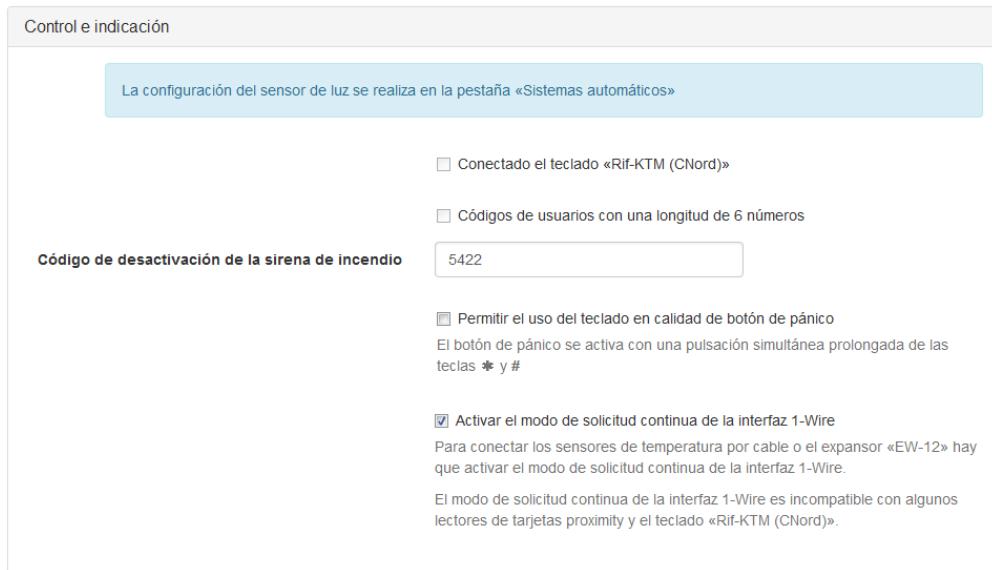
Se considera código de desarme forzado el código que se diferencia del código del usuario en una unidad en dirección mayor o menor. Por ejemplo, si el código del usuario es «1234», los códigos de desarme forzado serán «1233» y «1235». Teniendo en cuenta:

- si el código del usuario termina con el número «0», el código de desarme forzado solo será uno – en una unidad superior. Por ejemplo, si el código del usuario es igual a «5840», el código de desarme forzado sólo será el código «5841».
- si el código del usuario termina con el número «9», el código de desarme forzado también será solo uno – en una unidad inferior. Por ejemplo, si el código del usuario es igual a «5849», el código de desarme forzado sólo será el código «5848».

No iniciar el retraso de salida en el CN-K

Debido a que el teclado “CN-K” es inalámbrico y funciona con baterías, la desactivación de la indicación de retraso de entrada permite aumentar el tiempo de funcionamiento de las baterías en el teclado “CN-K”.

5.6.3 Control e indicación



Puc. 63: Pestaña «Varios», apartado «Control e indicación»

La configuración del avisador óptico se realiza en la pestaña “Sistema automático”

Para que el usuario pueda controlar de forma visual el estado de la alarma de seguridad en el objeto, al equipo se puede conectar un avisador óptico con una tensión de alimentación de 12 V. La configuración de este avisador se realiza en el apartado [Sistema automático](#).

Conectado el teclado “Rif-KTM (C-Nord)”

Si se usa el teclado inalámbrico “Rif-KTM (C-Nord)”, hay que marcar la correspondiente casilla, para que la indicación del teclado funcione correctamente.

Códigos de usuarios con una longitud de 6 números

Para usar códigos de seis números para armar o desarmar el sistema de seguridad, primero hay que establecer este parámetro y a continuación crear usuarios. Si en el dispositivo ya existen usuarios con un código de seis números, primero hay que eliminarlos y a continuación establecer el parámetro para usar códigos de seis números.

Permitir el uso del teclado en calidad de botón de emergencia

Para usar el teclado en calidad de botón de emergencia, hay que marcar la correspondiente casilla

- Para los teclados “K14-LED” y “CN-K” el botón de emergencia se activa con una pulsación simultánea prolongada de los botones con la imagen de la casita.
- Para el teclado “K16-LCD” el botón de emergencia se activa con una pulsación prolongada de los botones asterisco y almohadilla.

Activar el modo de solicitud continua de la interfaz 1-Wire

El modo de solicitud continua 1-Wire hay que activarlo si al equipo están conectados sensores de temperatura por cable o el expansor “EW-12”. Este modo no es compatible con algunos lectores de tarjetas proximity y el teclado “Rif-KTM (C-Nord)”.

5.6.4 Protección de la configuración

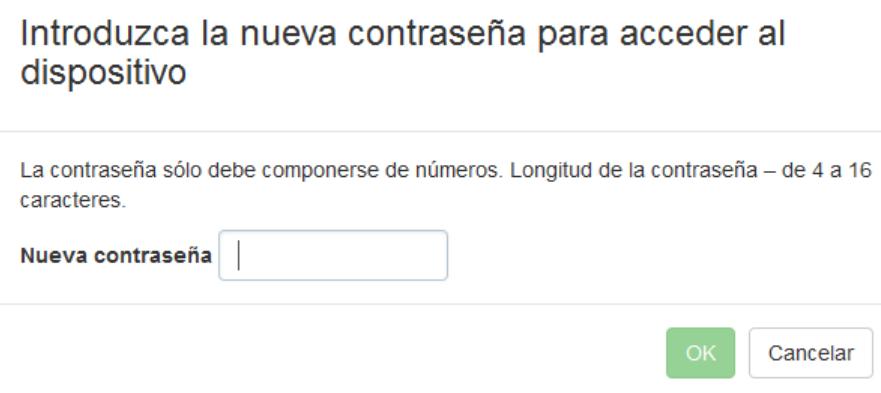
Mediante este apartado se pueden configurar los parámetros para la protección contra acceso no sancionado e introducción de cambios malintencionados en los parámetros de los equipos.



Puc. 64: Pestaña «Varios», apartado «Protección de la configuración»

Contraseña para acceder al equipo

Una autentificación obligatoria a través de la contraseña al conectarse al equipo por USB es una forma más de garantizar la seguridad. De forma predeterminada la contraseña para la conexión al equipo por USB es **0000**. Para elevar la seguridad, hay que cambiar la contraseña de acceso estándar por una nueva. La longitud de la contraseña puede ser de 4 a 16 números. Se recomienda establecer una contraseña compuesta de la máxima cantidad permitida de números.



Puc. 65: Pestaña «Varios», apartado «Protección de la configuración», diálogo para cambiar la contraseña para acceder al equipo.

Si la contraseña fue perdida y no es posible conectarse al equipo de forma remota, sólo se puede recuperar el acceso al equipo resemando los valores de todos sus parámetros a los parámetros de fábrica. Con ello serán eliminadas todas las configuraciones del equipo, incluyendo las zonas, los usuarios, las particiones, etc., y la contraseña para la conexión al equipo por USB volverá al valor predeterminado.

Permitir el reseteo de los valores de los parámetros a los parámetros de fábrica

La función de reseteo de los valores se puede activar o desactivar para un equipo en concreto. Permitiendo el reseteo de los valores de los parámetros, se puede establecer una **pausa antes del reseteo**. De forma predeterminada este parámetro está establecido por 30 segundos, sin embargo se puede elegir un valor de 5 minutos, 30 minutos, 12 horas o 24 horas. Sólo es posible resetear la configuración conectándose por USB.

Si la función de reseteo de la configuración está activada, la ventana para la introducción de la contraseña tendrá el botón “Resetear la configuración”

Introduzca la contraseña para acceder al dispositivo

Número de serie: 38724075

Contraseña

Resetear la configuración

OK

Puc. 66: Pestaña "Varios apartado "Protección la configuración diálogo para resetear la configuración del equipo.

Al pulsar el botón "Resetear la configuración" el equipo crea un evento con el código **E752** y empieza la cuenta de la pausa establecida.

Se recomienda establecer el valor máximo del parámetro *Pausa antes del reseteo*, ya que tal retraso proporciona seguridad adicional. Si la configuración del dispositivo la resetea un malhechor, a la empresa de seguridad privada le da tiempo de reaccionar a un acceso no sancionado al equipo.

Activar la función “Protección de cambio de servicio”

Si esta función está activada y los cambios fueron guardados en el equipo, para este equipo ya no se podrán cambiar los valores de los siguientes parámetros:

- direcciones para la conexión a través de GPRS;
- direcciones para la conexión a través de Ethernet;
- formato de estación para la transmisión por radio.

Antes de guardar la configuración en el equipo se muestra la advertencia:

Protección de cambio de servicio

En la configuración que quiere grabar en el dispositivo, está incluida la función «Protección de cambio de servicio».

Después de que la configuración sea guardada, los valores de los siguientes parámetros no se podrán modificar:

- direcciones para la conexión al «Security center» por GPRS;
- formato de la estación para la transmisión por radio.

¿Está seguro de que quiere grabar la configuración en el dispositivo?

Grabar

Cancelar

Puc. 67: Pestaña «Varios», apartado «Protección de la configuración», advertencia de activación de la "Protección de cambio de servicio".

La función “protección de cambio de servicio” puede activarse al conectar por USB y también bajo programación remota. La función “Protección de cambio de servicio” se puede desconectar únicamente poniéndose en [contacto con el soporte técnico](#) mediante una solicitud oficial a “C-Nord”.

5.7 Security Center

En la pestaña “Security Center” se pueden indicar los parámetros que usará el equipo al transmitir eventos a la consola de seguridad a través de los canales GSM y Ethernet.

5.7.1 Identificación del equipo

Puc. 68: Pestaña «Security center», apartado «Identificación»

En el apartado “Identificación” se puede especificar el número del objeto que se usará durante la transmisión de eventos desde el equipo.

Debido a que la transmisión de eventos desde el equipo en el software del “Security Center” se realiza en el protocolo que es un equivalente informático al protocolo Ademco ContactID, cada evento, si es posible, contiene la información del número de la partición en la cual tuvo lugar, así como del número de la zona que generó la creación del evento, o el número del usuario que realizó el arme o desarme de la partición. De esta forma, al transmitir a través de GSM o Ethernet un numero del objeto es suficiente para trasmitir cualesquiera eventos desde el equipo sin pérdida de sus características informativas.

En el apartado “Identificación”, en el campo “Identificador del dispositivo” se muestra un número de serie único de ocho dígitos asignado al dispositivo durante la fabricación. Este número de serie puede transmitirse a la consola de seguridad y servir en calidad de alternativa al número del objeto al identificar el equipo. Para activar esta posibilidad sirve el parámetro “Trasmitir el identificador del dispositivo al programa de la consola”. En el software del “Security Center” la posibilidad de usar el número de serie del equipo en vez del numero del objeto no está realizada: si la transmisión del número de serie al programa de la consola está activada, el número de serie simplemente se mostrará en la tarjeta del objeto en la pestaña “Equipos”.

Si en calidad del software de la consola se usa el “Security Center” de la versión 4, no se puede trasmitir el número de serie al programa de la consola: el equipo no podrá conectarse al “Security Center”.

Para que los eventos desde el equipo se procesen correctamente por el software del “Security Center”, deben cumplirse las siguientes condiciones:

- el numero del objeto, asignado al configurar el equipo, debe coincidir con el numero del objeto, creado para el equipo en el software del “Security Center”;
- en el módulo “Administrador de objetos”, en el apartado “Equipos” para este objeto debe indicarse el valor “C-Nord GSM (CML)”;
- antes de la primera conexión del equipo al software del “Security Center” hay que asegurarse que el valor en el campo “Identificador” en la pestaña “Equipos” no está asignado.

Puc. 69: Módulo «Administrador de objetos», pestaña «Equipos»

5.7.2 Parámetros de transmisión por GPRS



Puc. 70: Pestaña «Security Center», apartado «Transmisión por TCP/IP (GPRS)»

En el apartado “Transmisión por TCP/IP (GPRS)” se pueden asignar hasta dos pares “dirección:puerto”, que se usarán por el equipo al conectarse a la consola de seguridad a través de los canales GSM/GPRS.

En calidad de valores a los campos “Dirección 1” y “Dirección 2” se puede indicar tanto la dirección IP, como el nombre DNS.

Al inicializar la conexión a través de GPRS, el equipo primero intenta conectarse al servidor con los parámetros “Dirección1:Puerto 1”. Si no se consigue establecer la conexión, se realizará el intento de conectar al servidor con los parámetros “Dirección 2:Puerto 2”. Con ello ambos pares “dirección:puerto” se perciben por el equipo como equivalentes: la diferencia entre ellos sólo consiste en qué par se utilizará para la inicialización de la conexión primera. Si el equipo se conecta a la consola de seguridad usando los pares “Dirección 2:Puerto 2”, esa conexión no se considerará conectada a través del canal de reserva y sólo será cerrada si se pierde la conexión con la consola de seguridad con el uso de esta conexión..

Ambos pares “dirección:puerto” son válidos para ambas tarjetas SIM, instaladas en el equipo: independientemente de cuál de las tarjetas SIM actualmente está activa, el equipo primero realizará el intento de conexión a la consola de seguridad con los parámetros “Dirección 1:Puerto 1” y sólo si este intento falla - intentará conectar con los parámetros “Dirección 2:Puerto 2”.

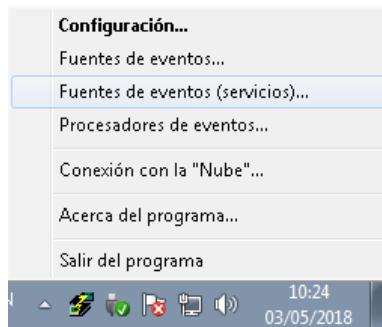
En caso de que en la consola de seguridad sólo haya una dirección para la conexión de equipos a través de TCP/IP, al configurar el equipo los valores para los parámetros “Dirección 2:Puerto 2” hay que dejarlos en blanco.

Si al equipo no está conectado el módulo opcional “Adaptador Ethernet”, el canal GSM/GPRS en la SIM1 se considera principal para el equipo.

Recepción de eventos en el “Security Center”

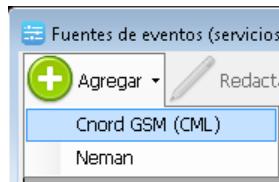
Para recibir eventos del equipo a través de los canales TCP/IP (GSM/GPRS y Ethernet) en el software del “Security Center” hay que usar la fuente de eventos “C-Nord GSM (CML)”. Esta fuente de eventos se puede añadir o modificar sus parámetros en el módulo “Administrador de eventos”.

Para abrir la ventana de configuración del servicio de las fuentes de eventos hay que seleccionar el punto “Fuentes de eventos (servicios)...” en el menú contextual que aparecerá al pulsar el botón derecho del ratón sobre el ícono del módulo en la parte del sistema del panel de tareas.



Puc. 71: Menú contextual del módulo «Administrador de eventos»

Para añadir la fuente de eventos de «C-Nord GSM (CML)» al servicio de fuentes de eventos, hay que pulsar el botón “Añadir” y seleccionar el punto, fuente correspondiente, en el menú que aparezca.



Puc. 72: Menú da la ventana de configuración del servicio de fuentes de eventos

Fuente de eventos

Nombre	Puerto - 2118, canal GPRS
Descripción	Fuente de eventos para consolas "Nord GSM", "Serzhant GSM", "Soyuz GSM" y transmisores "TP-100 GSM III", que utilizan el protocolo de transmisión CML
Interfaz de red	0.0.0.0
Puerto	2118
Número interno del objeto	9000
Tipo de canal de comunicación	GPRS
Número de canal de comunicación	1
Desplazamiento de números de objetos	0
Intervalo de ping (seg.)	90
<input checked="" type="checkbox"/> Fuente activada	
<input type="button" value="Guardar"/> <input type="button" value="Cancelar"/>	

Puc. 73: Ventana de configuración de la fuente de eventos «C-Nord GSM (CML)»

Puede leer con más detalle sobre las asignaciones de los parámetros de la fuente de eventos «C.Nord GSM (CML)» en la documentación del software del “Security Center”.

¿Dirección IP o nombre DNS?

En calidad de dirección del servidor se recomienda especificar el nombre DNS y no la dirección IP, por el siguiente motivo. La dirección IP dedicada, como norma, le pertenece concretamente al operador de comunicación que proporciona el acceso a Internet y no puede ser pasada a la conexión, proporcionada por otro operador de comunicación. Lo que respecta al nombre DNS, este le pertenece a la organización que lo registró, por ejemplo a la empresa de seguridad. Aparte de esto, la correspondencia del nombre DNS y la dirección IP también la asigna la empresa de seguridad.

¿Qué pasará, si por algún motivo se deberá rescindir el contrato con el operador de comunicación que le proporciona a la empresa de seguridad el acceso a Internet? Si en calidad de dirección para la conexión a la consola de seguridad está indicado el nombre DNS, será suficiente con cambiar el registro que asigna la correspondencia del nombre DNS y la dirección IP. En el caso de que esté indicada la dirección IP, habrá que dirigirse a cada objeto para cambiar el valor de la dirección.

Partiendo de lo especificado *recomendamos insistentemente* usar precisamente el nombre DNS y no la dirección IP.

5.7.3 Parámetros de transmisión por Ethernet

Transmisión por TCP/IP (Ethernet)

Dirección 1	10.7.0.222	Puerto 1	1036
Dirección 2		Puerto 2	0

Puc. 74: Pestaña «Security Center», apartado «Transmisión por TCP/IP (Ethernet)»

En el apartado “Transmisión por TCP/IP (Ethernet)”, al igual que en el anterior apartado se pueden asignar dos pares “dirección:puerto”, que se usarán por el dispositivo al conectarse a la consola de seguridad a través del canal

Ethernet. Todos los comentarios hechos en relación a los pares “dirección:puerto” en la descripción del apartado “Transmisión por TCP/IP (GPRS)” se extienden también sobre los parámetros en el apartado “Transmisión por TCP/IP (Ethernet)”.

En el caso general los valores de los parámetros “dirección:puerto” deben ser similares para los apartados “Transmisión por TCP/IP (GPRS)” y «Transmisión por TCP/IP (Ethernet)». Sin embargo, en algunos casos estos valores pueden ser diferentes. Por ejemplo, si para el canal GSM/GPRS se usa una conexión VPN protegida, proporcionada por el operador de comunicación móvil, las direcciones de conexión a través de GSM/GPRS y Ethernet pueden ser diferentes, ya que la conexión a través de Ethernet se realizará a través de una red pública. Pero incluso en este caso se puede organizar la conexión a través del canal GSM/GPRS de una forma que en calidad de dirección de la consola se use el nombre DNS y no la dirección IP.

Si al equipo está conectado el módulo opcional “Adaptador Ethernet”, entonces el canal Ethernet se considera *principal* para el equipo.

El apartado “Transmisión por TCP/IP (Ethernet)” se muestra en el configurador sólo si al equipo está conectado el módulo opcional “Adaptador Ethernet”.

5.7.4 Parámetros de transmisión en el canal CSD GSM

Transmisión en canal CSD GSM			
Número 1 para la SIM 1	<input type="text"/>	Número 1 para la SIM 2	<input type="text"/>
Número 2 para la SIM 1	<input type="text"/>	Número 2 para la SIM 2	<input type="text"/>

Puc. 75: Pestaña «Security Center», apartado «Transmisión en el canal CSD GSM»

En el apartado “Transmisión en el canal CSD GSM” se pueden especificar los números de teléfonos que se usarán para llamar a la consola de seguridad al transmitir eventos en el canal CSD GSM.

A diferencia de los canales GSM/GPRS y Ethernet, los números de teléfonos para la transmisión en el canal CSD se asignan de forma separada para cada SIM. Esto se debe a que el coste del servicio de transmisión por CSD dentro de la red del operador de comunicación puede ser considerablemente menor.

Al transmitir en el canal CSD el dispositivo primero realiza una llamada al primer número, indicado para la tarjeta SIM activa actualmente y si la transmisión del evento no tuvo éxito, a través del segundo. Si en la consola de seguridad sólo está instalado un modem para la recepción de eventos por el canal CSD, el segundo número de teléfono hay que dejarlo en blanco.

El canal CSD se considera activo si está asignado aunque sea un número de teléfono. Si el equipo no debe usar el canal CSD para la transmisión de eventos, ambos números de teléfono deben estar en blanco.

Recepción de eventos en el “Security Center”

Para recibir eventos del equipo a través del canal CSD en el software del “Security Center” hay que usar la “Fuente de eventos por GSM”. Esta fuente de eventos se puede añadir o modificar sus parámetros en el módulo “Administrador de eventos”

En calidad de equipo para la recepción de eventos por el canal CSD puede usarse cualquier modem GSM, cuyo sistema de comandos es compatible con el modem Siemens MC35.

5.7.5 Parámetros de transmisión en el canal de voz GSM

Transmisión en canal de voz GSM			
Número 1 para la SIM 1	<input type="text"/>	Número 1 para la SIM 2	<input type="text"/>
Número 2 para la SIM 1	<input type="text"/>	Número 2 para la SIM 2	<input type="text"/>

Puc. 76: Pestaña «Security Center», apartado «Transmisión en el canal de voz GSM»

En el apartado “Transmisión en el canal de voz GSM” se pueden especificar los números de teléfonos que se usarán para llamar a la consola de seguridad al transmitir eventos en el canal de voz GSM. La transmisión en el canal de voz se realiza mediante las señales analógicas DTMF, en calidad de protocolo informático se usa Ademco Contact ID.

Los números de teléfonos para la transmisión en el canal de voz se asignan de forma separada para cada SIM, ya que la llamada por voz dentro de la red del operador de comunicación puede ser más barata.

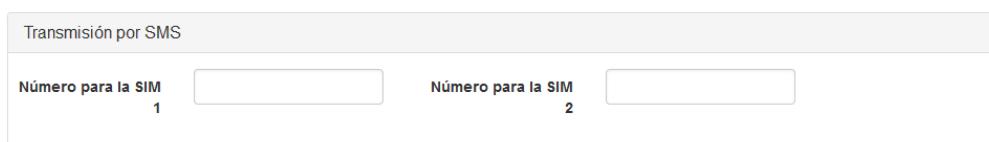
Al transmitir en el canal de voz el equipo primero realiza una llamada al primer número, indicado para la tarjeta SIM activa actualmente y si la transmisión del evento no tuvo éxito, a través del segundo. Si en la consola de seguridad sólo hay un número para la recepción de llamadas por voz, el segundo número de teléfono hay que dejarlo en blanco.

El canal GSM por voz se considera activo si está asignado aunque sea un número de teléfono. Si el equipo no debe usar el canal por voz para la transmisión de eventos, ambos números de teléfono deben estar en blanco.

Recepción de eventos en el “Security Center”

Para recibir eventos del equipo a en el canal GSM por voz hay que usar un equipo de consola especialmente destinado para tal fin. En calidad de ejemplo de tal equipo se puede poner el procesador de la estación central “Sentinel” de fabricación de la compañía “Pima Electronics” o los procesadores de la estación central “SG System III” / “SG System IV” de fabricación de la compañía “DSC”.

5.7.6 Parámetros de transmisión por SMS



Puc. 77: Pestaña «Security Center», apartado «Transmisión por SMS»

En el apartado “Transmisión por SMS” se pueden especificar los números de teléfonos que se usarán para la transmisión de eventos a la consola de seguridad mediante el canal SMS.

Al transmitir por el canal SMS el equipo usa un protocolo que permite transmitir en un mensaje SMS hasta 5 eventos. Este protocolo sirve exclusivamente para la transmisión de información a la consola de seguridad y no puede ser usado para informar a los usuarios sobre los eventos en el objeto.

El número de teléfono para la transmisión por el canal SMS se especifica de forma separada para cada SIM, ya que el envío de SMS dentro de la red del operador de comunicación puede ser más barato.

El canal SMS se considera activo si tiene asignado un número de teléfono. Si el equipo no debe usar el canal SMS para la transmisión de eventos, el número de teléfono debe estar en blanco.

Recepción de eventos en el “Security Center”

Para recibir eventos del equipo en el canal SMS en el software del “Security Center” hay que usar la “Fuente de eventos por GSM”. Esta fuente de eventos se puede añadir o modificar sus parámetros en el módulo “Administrador de eventos”

En calidad de equipo para la recepción de eventos por el canal SMS puede usarse cualquier modem GSM, cuyo sistema de comandos es compatible con el modem Siemens MC35.

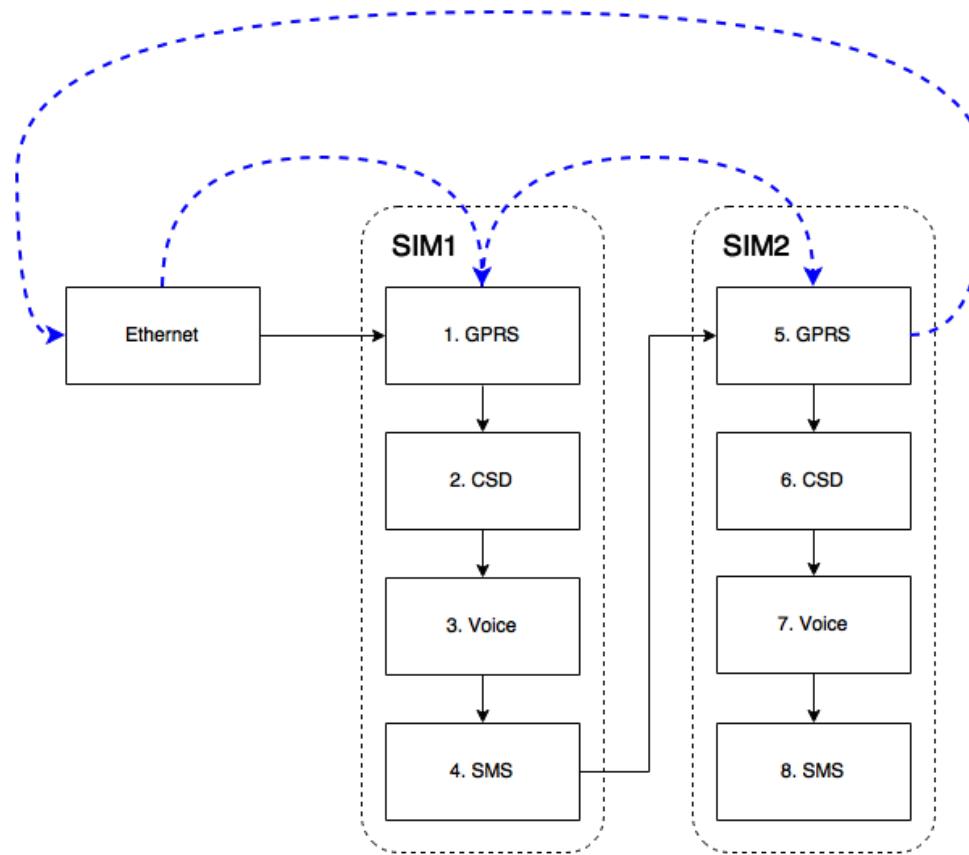
5.7.7 Cambio de canales de comunicación

Para determinar el siguiente canal de comunicación, si el canal IP actual no funciona, sirve la siguiente regla:

- si no hay eventos de transmisión, se realiza el cambio a otro canal IP. Por ejemplo, si no funciona el GPRS en la SIM1, el dispositivo pasará al GPRS en la SIM2 y viceversa;
- si el evento tiene lugar, se realiza el intento de su transmisión mediante el canal de reserva en aquella SIM que ahora está activa. Al finalizar el envío de eventos se reanuda el intento de conexión a través de los canales IP.

Si la transmisión en los canales de reserva de la SIM1 no se pudo realizar, se realizará el cambio a la SIM2 y la selección de canales allí.

Si no hay eventos para la transmisión, el equipo irá seleccionando los canales IP hasta que realice la conexión, o hasta que no aparezca un evento para la transmisión. Es importante que el equipo puede diferenciar la situación “GPRS no funciona” de la situación “no hay conexión al “Security Center”. En el primer caso se realiza el cambio a otro canal IP, en el segundo caso continúan los intentos de conectarse a la consola dentro de una sesión GPRS.



Puc. 78: Esquema de cambio de canales de comunicación

El orden de cambio de los canales de comunicación IP en caso de no haber eventos se muestra en el dibujo con líneas azules intermitentes. Con líneas negras continuas se muestra el esquema de cambio de todos los canales configurados en caso de haber eventos para la transmisión.

5.8 Radio

“Nord GSM” puede transmitir eventos a la consola de seguridad no sólo a través de los canales GSM y Ethernet, sino también por el canal de radio. La transmisión por radio puede realizarse en modo duplicado, cuando todos los eventos siempre se envían por radio, tanto en modo de reserva, cuando los eventos por radio se transmiten si no hay comunicación IP con la consola de seguridad.

La transmisión por radio se realiza *sólo* en el protocolo «EPAF», el protocolo «PAF» no se soporta.

5.8.1 Configuración del canal de radio

Configuración del canal de radio	
Modo de uso	Transmitir al no haber comunicación IP
Formato de estación	34560
Cantidad de secuencias en un envío	5
Cantidad de secuencias en un paquete	10
Intervalo entre paquetes, seg.	5
Intervalo de transmisión de pruebas, min.	90

Puc. 79: Pestaña «Radio», apartado «Configuración del canal de radio»

En el apartado "Configuración del canal de radio" se asignan los parámetros que usará el equipo al transmitir eventos por radio.

Mediante el valor para el parámetro “Modo de uso” se puede especificar el modo en el cual se realiza la transmisión por radio:

- “Transmisor no conectado” - no se realizará la transmisión por radio;
- “Transmitir si no hay comunicación IP” - la transmisión por radio se realizará sólo si el equipo no tiene conexión a la consola de seguridad a través de los canales de comunicación IP (Ethernet o GPRS);
- “Trasmitir siempre” - todos los eventos creados por el equipo siempre se transmitirán por radio.

El parámetro “Formato de la estación” asigna la clave que se usa al realizar la codificación de los envíos al enviar por radio. El formato para cada estación «CMS-420» / «Sentinel» se asigna por el fabricante al suministrar la estación y está indicado en su documentación adjunta.

Debido a que durante la transmisión por radio no hay confirmaciones de recepción de eventos por parte de la estación, el equipo del objeto transmite el mismo evento muchas veces. La información codificada para la transmisión por radio que corresponde al evento se llama secuencia. Varias secuencias que se transmiten en serie, sin pausa entre ellas, se llaman paquete. Varios paquetes que se envían a la estación con pausa entre ellos se llaman envío. De esta forma, al transmitir por radio, cada evento se transmitirá en forma de un envío, los parámetros para crear el cual se pueden especificar.

Para controlar el funcionamiento del canal de transmisión por radio sirve el parámetro “Intervalo de transmisión de pruebas”. Mediante este parámetro se puede asignar el intervalo máximo, al transcurrir el cual, del equipo debe recibirse cualquier evento por radio. Este intervalo siempre se cuenta a partir del último evento que fue transmitido por radio. Si al transcurrir el intervalo no habrá eventos que hay que transmitir por radio, se creará y se transmitirá un evento de prueba.

Hay que entender que los eventos de prueba con intervalo establecido se transmiten independientemente de la existencia de comunicación IP con la consola de seguridad: incluso si el canal de transmisión por radio se usa como de reserva y la transmisión de eventos por radio se realiza sólo si no hay comunicación IP con la consola de seguridad, los eventos de prueba se transmitirán con el intervalo especificado.

5.8.2 Números de particiones de los objetos

Números de objetos de las particiones	
Partición	Número del objeto
1	2007
2	2008
3	2009

Puc. 80: Pestaña «Radio», apartado «Números de particiones de los objetos»

Debido a que el protocolo de transmisión por radio no permite usar los números de las particiones, para cada partición del panel de control hay que especificar un número de objeto que se usará al transmitir por radio.

Recomendamos insistentemente especificar tales números de particiones de los objetos, que no coincidan ni con el número del objeto que se asigna en la pestaña “Security Center”, ni con los números de objetos de otras particiones. Esto hace falta para que los eventos creados por la partición puedan diferenciarse de los eventos de servicio, creados por el equipo, y aparte de esto, de los eventos creados por otra partición.

5.8.3 Equipo en cuerpo metálico

Si se prevé que el panel de control funcionará por radio, se suministrará en cuerpo metálico. Por una parte, el cuerpo metálico tiene grandes dimensiones en comparación con el cuerpo de plástico. Pero por otra parte, estas dimensiones le ofrecen una serie de ventajas, inclusive al usar el canal de radio:

- hay sitio para la instalación del transmisor de radio;
- el cuerpo mismo sirve de contrapeso para la antena de látilo;
- se prevé la posibilidad de instalar un expansor por cable y un expansor inalámbrico «CN-RADIO». De esta forma, al equipo “Nord GSM” en cuerpo metálico se pueden conectar hasta 16 zonas por cable y hasta 31 dispositivo inalámbrico;
- se puede instalar una batería de mayor capacidad - hasta 7.2 A * h.

5.9 Nube

La conexión del equipo a la “Nube” proporciona el funcionamiento de las funciones de servicio del equipo y permite interactuar de forma remota con el mismo, mediante la aplicación móvil «MyAlarm» y el servicio “Panel del técnico”. La descripción detallada de la tecnología se encuentra en el apartado [Acceso remoto al equipo..](#)

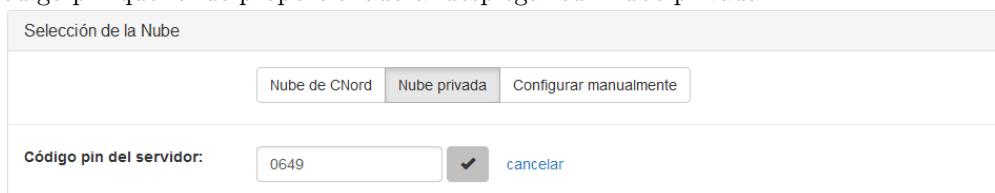
En la pestaña “Nube” se puede seleccionar a qué “Nube” precisamente debe conectarse el equipo.

Si para el funcionamiento usa la “Nube de C-Nord” pública, todo es fácil - simplemente hay que pulsar el botón con el mismo nombre:



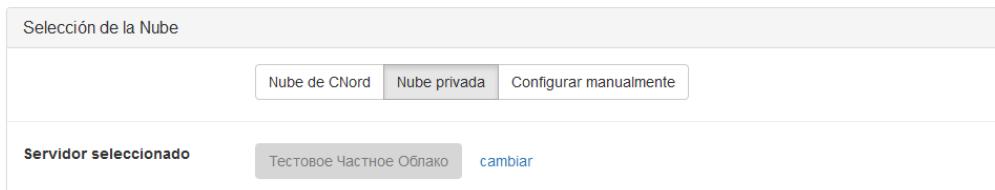
Puc. 81: Pestaña "Nube seleccionado el uso de "Nube" pública.

Si el equipo debe funcionar con una “Nube privada”, hay que pulsar el botón “Nube privada”, a continuación introducir el código pin que le fue proporcionado al desplegar su “Nube privada”:



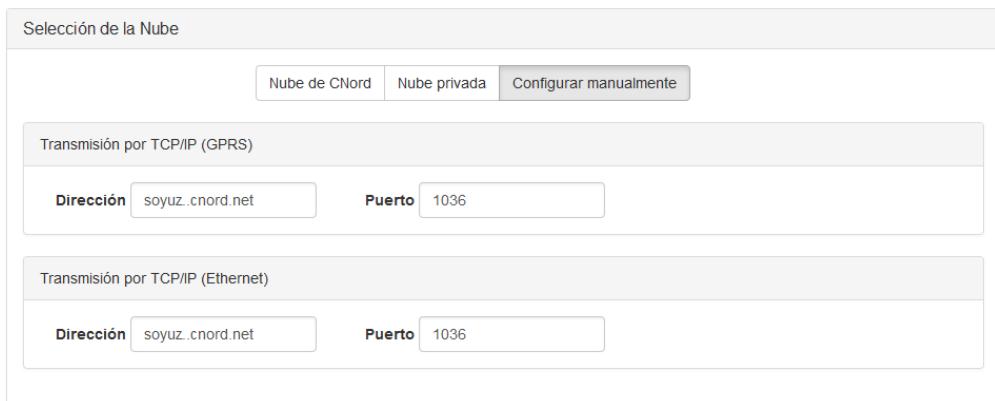
Puc. 82: Pestaña "Nube seleccionado el uso de "Nube privada".

Si el código pin del servidor de la “Nube privada” se introduce correctamente, al pulsar el botón con la “casilla marcada” en vez del campo de introducción se mostrará el nombre de la “Nube privada” que corresponde al código pin:



Puc. 83: Pestaña "Nube se muestra el nombre de la "Nube privada".

Si por algún motivo hay que realizar una configuración para la conexión a la “Nube privada” manualmente, puede hacerlo: hay que pulsar el botón “Configuración manual” y especificar las direcciones y los puertos para la conexión a la “Nube” a través de los canales GPRS y Ethernet (se muestra sólo si el adaptador Ethernet está conectado al equipo):



Puc. 84: Pestaña "Nube configuración de los parámetros para la conexión manual.

5.10 Ethernet

La pestaña sirve para mostrar y cambiar la configuración de la conexión a través de la red Ethernet.

La pestaña “Ethernet” se muestra en el configurador sólo si el dispositivo «Adaptador Ethernet» está conectado al equipo.

En la pestaña se muestra la dirección MAC que se usa por el dispositivo «Adaptador Ethernet». Esta información puede ser útil, si la configuración para la conexión a la república se realiza de forma individual para cada dispositivo.

Parámetro del módulo Ethernet

Dirección MAC: 00:1E:C0:84:34:C5	
<input checked="" type="checkbox"/> Recibir la configuración por DHCP	
Dirección IP local	
Máscara de subred	
Dirección IP de puerta de enlace	
DNS principal	
DNS secundario	

Puc. 85: Pestaña "Ethernet activado el modo de recepción de configuraciones del servidor DHCP".

A parte de esto, si la red a la cual está conectado el equipo no dispone de un servidor DHCP que proporciona la configuración automática de los parámetros de conexión a la red, estos parámetros se pueden asignar manualmente, indicando expresamente la dirección IP que debe usar el equipo, la máscara de subred a la cual pertenece el equipo, la dirección IP de la puerta de enlace que debe usarse para el acceso a la red pública, así como la dirección IP de los servidores DNS.

Parámetro del módulo Ethernet

Dirección MAC: 00:1E:C0:84:34:C5	
<input type="checkbox"/> Recibir la configuración por DHCP	
Dirección IP local	192.168.1.154
Máscara de subred	255.255.255.0
Dirección IP de puerta de enlace	192.168.1.1
DNS principal	8.8.8.8
DNS secundario	

Puc. 86: Pestaña "Ethernet configuración manual de la red".

5.11 Operadores GSM

Mediante la pestaña “Operadores GSM” en el equipo se graba la información necesaria para el correcto funcionamiento de las tarjetas SIM en la red GSM.

<p>Operador 1</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Nombre</td> <td>MEGAFON</td> </tr> <tr> <td>Número de la red (PLMN)</td> <td>25002</td> </tr> <tr> <td>Punto de acceso</td> <td>internet</td> </tr> <tr> <td>Nombre del usuario</td> <td></td> </tr> <tr> <td>Contraseña</td> <td></td> </tr> </table>	Nombre	MEGAFON	Número de la red (PLMN)	25002	Punto de acceso	internet	Nombre del usuario		Contraseña		<p>Operador 2</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Nombre</td> <td>MTS</td> </tr> <tr> <td>Número de la red (PLMN)</td> <td>25001</td> </tr> <tr> <td>Punto de acceso</td> <td>internet.mts.ru</td> </tr> <tr> <td>Nombre del usuario</td> <td>mts</td> </tr> <tr> <td>Contraseña</td> <td>mts</td> </tr> </table>	Nombre	MTS	Número de la red (PLMN)	25001	Punto de acceso	internet.mts.ru	Nombre del usuario	mts	Contraseña	mts
Nombre	MEGAFON																				
Número de la red (PLMN)	25002																				
Punto de acceso	internet																				
Nombre del usuario																					
Contraseña																					
Nombre	MTS																				
Número de la red (PLMN)	25001																				
Punto de acceso	internet.mts.ru																				
Nombre del usuario	mts																				
Contraseña	mts																				
<p>Operador 3</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Nombre</td> <td>TELE2</td> </tr> <tr> <td>Número de la red (PLMN)</td> <td>25020</td> </tr> <tr> <td>Punto de acceso</td> <td>internet.tele2.ru</td> </tr> <tr> <td>Nombre del usuario</td> <td></td> </tr> <tr> <td>Contraseña</td> <td></td> </tr> </table>	Nombre	TELE2	Número de la red (PLMN)	25020	Punto de acceso	internet.tele2.ru	Nombre del usuario		Contraseña		<p>Operador 4</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Nombre</td> <td>BEELINE</td> </tr> <tr> <td>Número de la red (PLMN)</td> <td>25099</td> </tr> <tr> <td>Punto de acceso</td> <td>internet.beeline.ru</td> </tr> <tr> <td>Nombre del usuario</td> <td>beeline</td> </tr> <tr> <td>Contraseña</td> <td>beeline</td> </tr> </table>	Nombre	BEELINE	Número de la red (PLMN)	25099	Punto de acceso	internet.beeline.ru	Nombre del usuario	beeline	Contraseña	beeline
Nombre	TELE2																				
Número de la red (PLMN)	25020																				
Punto de acceso	internet.tele2.ru																				
Nombre del usuario																					
Contraseña																					
Nombre	BEELINE																				
Número de la red (PLMN)	25099																				
Punto de acceso	internet.beeline.ru																				
Nombre del usuario	beeline																				
Contraseña	beeline																				

Puc. 87: Pestaña "Operadores GSM configuraciones del operador.

De forma predeterminada en el configurador se enumeran los operadores de comunicación más extendidos. Antes de iniciar el equipo por GSM es importante asegurarse que están especificados los parámetros de la tarjeta SIM que se usa en el equipo. Si en los bloques enumerados no figuran los parámetros para el operador de comunicación seleccionando, hay que indicarlos manualmente, rellenando los campos *Nombre*, *PLMN*, *Punto de acceso*, *Nombre de usuario*, *Contraseña*. Todos estos parámetros el equipo puede solicitarlos a la tarjeta SIM durante el registro en la red.

5.12 Sistema automático

El mecanismo “Sistema automático” sirve para la programación del comportamiento del equipo dependiendo de unas u otras condiciones. En calidad de condiciones pueden actuar cualesquiera eventos, creados por el equipo o el tiempo. Y en calidad de acciones que el equipo puede realizar, actúan los armes o desarmes, así como las acciones con los colectores abiertos.

El sistema automático puede emplearse para la solución de las siguientes tareas en los objetos:

- arme y desarime de objetos por horario;
- arme y desarime de varias particiones al mismo tiempo;
- visualización del estado de la partición en el avisador óptico;
- activación de avisadores acústicos, conectados a los colectores abiertos del equipo;
- control de dispositivos exteriores, conectados a los colectores abiertos del equipo.

Al pasar a la pestaña “Sistema automático” arriba en la ventana se muestran los botones con los cuales se pueden configurar las reglas.



Los sistemas automáticos no están configurados

Puc. 88: Botones para la creación de reglas, pestaña «Sistema automático»

En el equipo ya está incluida la lógica de funcionamiento con avisadores ópticos y acústicos. Para la configuración de los colectores abiertos, a los cuales están conectados los avisadores, hay que usar los botones “Notificador...” o “Sirena...”, dependiendo del tipo del avisador.

Al crear las reglas es importante recordar las siguientes afirmaciones:

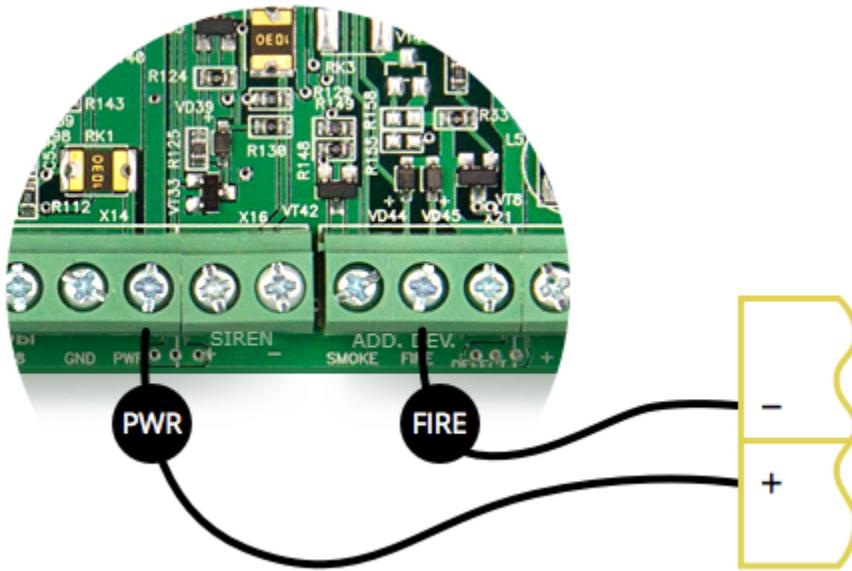
- Si el colector se usa para la conexión de otros dispositivos (por ejemplo, bloque de comunicación remota), entonces no se puede usar en ningún otro sitio, incluyendo el control remoto que aparecerá un poco más tarde.
- Si el colector ya se usa para los roles (notificador, sirena), no puede usarse en ningún otro sitio.
- Si al equipo está conectado el EW-12 y la zona del expansor está activada en la configuración del dispositivo, el colector en la zona no se puede usar para las reglas del sistema automático o para otros roles.
- En total se pueden crear 8 reglas con el rol “Notificador” o “Sirena”. Es de notar que estas normas no dependen de la cantidad de reglas estándares del sistema automático.

5.12.1 Notificador

Conexión del avisador óptico

Para conectar el notificador al equipo, hay que hacer lo siguiente:

- El cable “Positivo” del avisador conectarlo a cualquier salida positiva del panel de control, por ejemplo a la salida para la alimentación del teclado o las zonas.
- El cable “Negativo” del avisador debe conectarse a uno de los siete colectores abiertos: FIRE, DEFECT, LED_G, LED_Y, FIRE2, DEFECT2, DISABL.

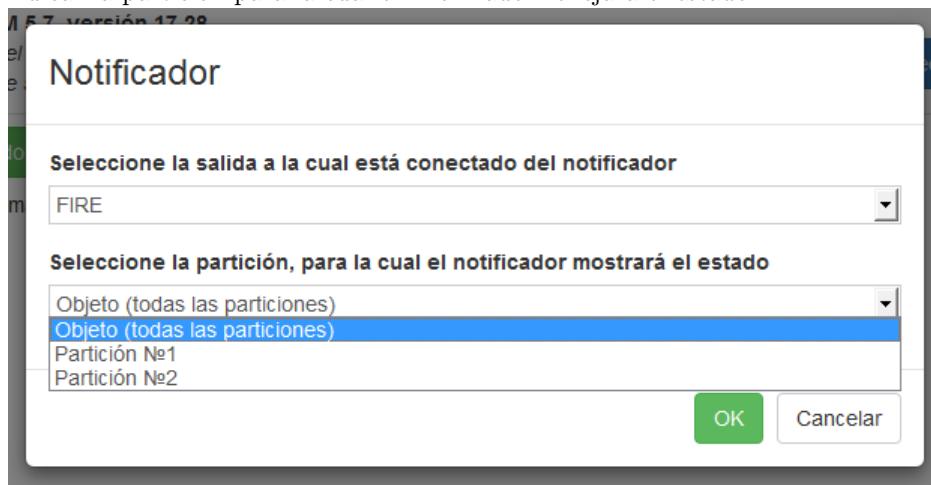


Puc. 89: Conexión del avisador óptico al dispositivo

Si al Nord está conectado el expansor EW-12, se pueden incorporar los bornes «Z1» - «Z8» del expansor. A los equipos se puede conectar cualquier avisador óptico con una tensión de alimentación de 12 V. La corriente máxima conmutada no debe superar los 250 mA.

Configuración de la regla

Para el avisador óptico que indica el estado del objeto o la partición hay que configurar la regla con el rol “Notificador”. Para crear la regla en la pestaña “Sistema automático” hay que pulsar el botón “Notificador” y seleccionar la salida a la cual está conectado el avisador. Si en el equipo hay varias particiones configuradas, al crear la regla hay que indicar la partición para la cual el informador reflejará el estado.



Puc. 90: Creación de la regla «Notificador»

Descripción del funcionamiento del avisador

Si la regla “Notificador” está configurada para mostrar el estado de la partición:

- El Notificador permanece encendido permanentemente, si la partición está armada;
- El Notificador no está encendido si la partición está desarmada;
- El Notificador parpadea si la partición está en situación de alarma;
- El Notificador parpadea con destellos dobles durante el retraso de la salida.

Si la regla “Notificador” está configurada para mostrar el estado del objeto:

- El Notificador permanece encendido permanentemente, si todas las particiones están armadas;
- El Notificador no está encendido si aunque sea una de las particiones está desarmada;
- El Notificador parpadea si aunque sea una de las particiones está en situación de alarma;
- El Notificador parpadea con destellos dobles durante el tiempo de retraso de la salida

5.12.2 Sirena

Conexión del avisador acústico

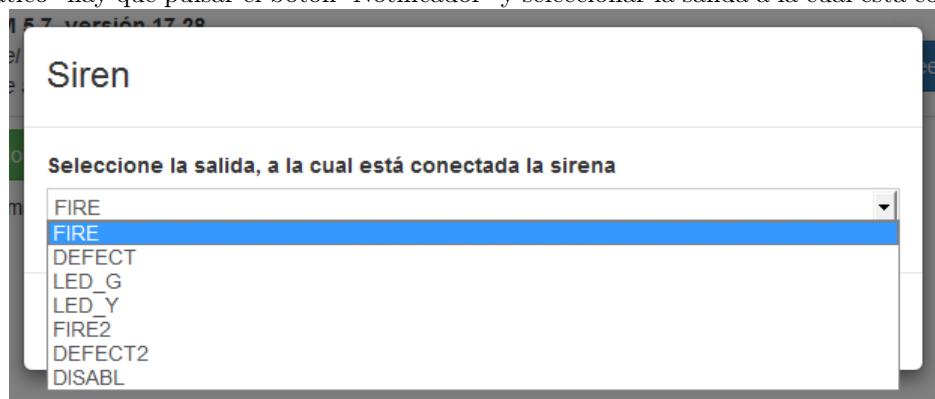
La conexión de la sirena al colector abierto se realiza de la siguiente forma:

- El cable “Positivo” del avisador puede ser conectado a cualquier salida positiva del panel de control, por ejemplo a la salida para la alimentación del teclado o las zonas.
- El cable “Negativo” del avisador debe conectarse a uno de los siete colectores abiertos: FIRE, DEFECT, LED_G, LED_Y, FIRE2, DEFECT2, DISABL.

Si al Nord está conectado el expansor EW-12, se pueden incorporar los bornes «Z1» - «Z8» del expansor. A los equipo se puede conectar cualquier avisador óptico con una tensión de alimentación de 12 V. La corriente máxima conmutada no debe superar los 250 mA.

Configuración de la regla

Para el avisador acústico hay que configurar la regla con el rol “Notificador”. Para crear la regla en la pestaña “Sistema automático” hay que pulsar el botón “Notificador” y seleccionar la salida a la cual está conectada la sirena.

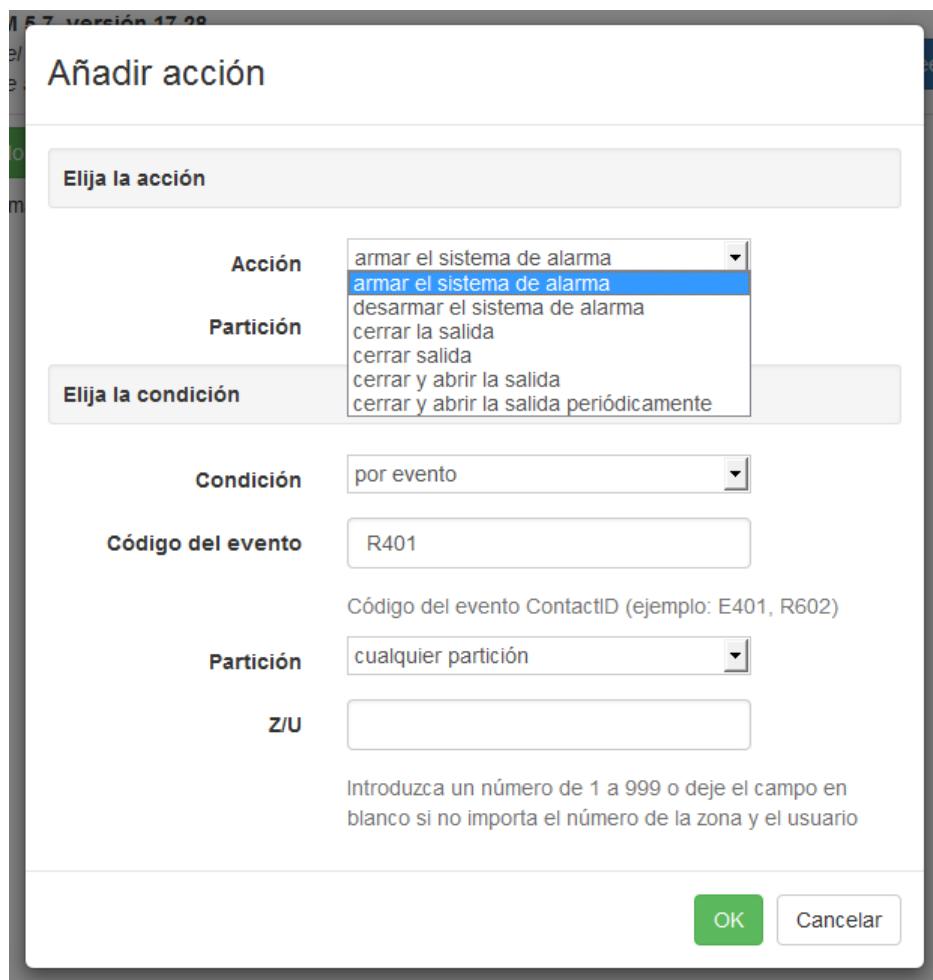


Puc. 91: Creación de la regla «Sirena»

La sirena conectada al colector abierto se diferencia de la sirena conectada a la salida del mismo nombre “Sirena” ya que en el primer caso el equipo no controla el estado de esta línea. Para configurar los parámetros del sonido de la sirena hay que ir al bloque [Sirena](#) de la pestaña Varios.

5.12.3 Varios

A parte de las reglas predeterminadas, en el equipo se pueden crear hasta 16 otras reglas. Al darse las condiciones especificadas en la regla, el equipo puede realizar el arme y el desarme de una o varias particiones, cerrar o abrir la salida discreta, así como empezar el cierre o la apertura periódica de la salida discreta con el intervalo especificado.



Puc. 92: Ventana de creación de la regla

Configuración de la regla

Analizaremos la configuración de las reglas en un ejemplo en concreto.

Objetivo

Configurar el arme de la partición Nº1 por horario a las 19 horas 30 minutos los martes y los miércoles.

Solución

Para la solución del objetivo planteado hay que crear una acción que realice el arme de la partición por horario.

1. En la pestaña “Sistema automático” pulsar el botón “Varios”.
2. En el campo “Acción” de la lista emergente seleccionar el valor “Armar el sistema de seguridad”
3. En el campo “Partición” seleccionar el valor “1”.
4. En el campo “Condición” seleccionar el valor “por horario”.
5. Mediante los menús emergentes en el campo “Tiempo” establecer el valor «19:30».
6. En el campo “Día de semana” seleccionar el valor “indicar”. En la lista de días de semana que apareció dejar marcadas las casillas “m” y “x”. Desmarcar las demás casillas.



Puc. 93: Ventana de creación de la regla

7. Pulse “OK” para guardar la regla. Las reglas entrarán en vigor después de guardar la configuración en el equipo.

Notificador...	Siren...	Otros...
Armar el sistema de alarma de la partición 1 por m, x en 06:30	Modificar...	Eliminar
Notificador conectado a la salida FIRE Muestra el estado de todo el objeto	Modificar...	Eliminar
Sirena activada a la salida LED_Y	Modificar...	Eliminar

Puc. 94: Todas las normas creadas

En el presente ejemplo se analiza el arme automático del sistema de seguridad, sin embargo en calidad de acción se puede indicar el desarme del sistema de seguridad del objeto. En este caso, el objeto se desarmará según el horario especificado. También se puede configurar el cierre y/o apertura automática de las salidas discretas del equipo.

Se puede configurar el arme de todas las particiones del objeto mediante el valor “Todas las particiones” el campo “Partición”. Para configurar el arme de varias particiones determinadas, para cada una hay que realizar la configuración del arme por separado.

El arme se puede asignar para días determinados de la semana, como en el ejemplo expuesto; para cada día; sólo para los días de semana (de lunes a viernes); también - sólo para los fines de semana.

El arme automático, al igual que cualquier otra acción, puede realizarse no sólo por horario, sino también por evento. En este caso hay que conocer el código del evento que se usará en la regla.

5.13 История событий

Вкладка предназначена для отображения событий, которые хранятся в энергонезависимой памяти прибора.

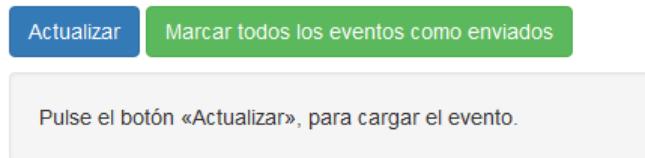


Рис. 95: Вкладка «История событий»

Для того чтобы загрузить события из прибора в конфигуратор, необходимо нажать на кнопку «Обновить».

Список событий, который отображается на вкладке «История событий», автоматически не обновляется: для того, чтобы увидеть, какие изменения произошли в истории событий с течением времени, необходимо нажать на кнопку «Обновить» еще раз.

Guardado en archivo...						
Tiempo	Código	Descripción	Objeto	Partición	Z / U	Enviado
04.05.2018 10:22:19	E321	Fallo de la sirena	3	0	0	GPRS a SIM1 04.05.2018 14:47:20
04.05.2018 10:07:19	E627	Activado el modo de programación (USB)	3	0	0	GPRS a SIM1 04.05.2018 14:34:10
04.05.2018 09:52:19	E137	Carcasa del equipo abierta	3	0	0	GPRS a SIM1 04.05.2018 14:34:09

Рис. 96: Вкладка «История событий», список событий

Объем энергонезависимой памяти прибора позволяет сохранить не менее 10.000 событий. Но на вкладке «История событий» отображается не более 200 последних событий. С помощью кнопки *Сохранить в файл..* можно выгрузить полный список событий в файл с расширением **.csv*.

При просмотре истории для каждого события отображается следующая информация:

- время, когда событие было сформировано прибором и сохранено в энергонезависимую память;
- код события, который передается на пульт охраны;
- текстовое описание события;
- номер объекта, для которого было сформировано событие;
- номер раздела;
- номер шлейфа или пользователя;
- информация о текущем состоянии события (колонка «Отправлено»):
 - если событие ожидает передачи, то отображается «прочерк»;
 - если событие отправлено на пульт охраны, то отображается информация о канале, который использовался для передачи события, а также время, когда было получено подтверждение о приеме события;
 - если отправка события была отменена из конфигуратора, то отображается информация об этом, а также время, когда была выполнена операция отмены передачи. Для того чтобы отменить передачу на пульт охраны всех событий, её ожидающих, нужно нажать на кнопку «Отметить события на устройстве, как отправленные».

При создании события оно получает уникальный порядковый номер. Порядок нумерации событий *не зависит* от времени, которое установлено на приборе: события, созданные ранее, имеют меньший номер, события, созданные позже – больший. На вкладке «История событий» события отображаются в порядке, обратном их номеру: события, созданные позже, отображаются выше, а события, созданные раньше – ниже по списку.

5.14 Панель состояния

При выполнении работ по монтажу объекта инженеру обычно нужно выполнить проверку, что размещение и подключение датчиков выполнено правильно и неисправностей в их работе нет.

В конфигураторе на вкладке “Панель состояния” отображается актуальная информация о состоянии проводных шлейфов, беспроводных устройств, подключенных к прибору, а так же состояние каналов связи.

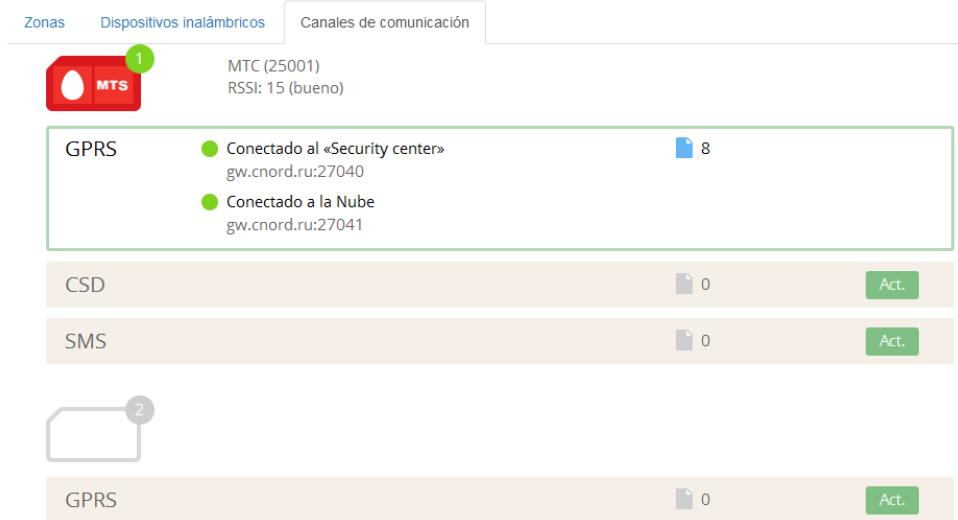


Рис. 97: Вкладка «Панель состояния», каналы связи

5.14.1 Каналы связи

При монтаже и обслуживании прибора важно знать актуальную информацию о состоянии каналов связи. С помощью вкладки “Панель состояния” можно видеть на какой SIM-карте и по какому каналу связи работает прибор в данный момент.

Для каждого канала связи, имеющегося в настройках прибора, отображается его текущее состояние: активен / не активен, есть ли подключение к «Центр охраны» и «Облаку», какие ошибки возникли при инициализации канала, подключении к пульту или передаче событий.

С помощью кнопки «Вкл.» можно выполнить принудительный переход на тот канал связи, работу которого нужно проверить. Для того чтобы инженер мог убедиться, что канал действительно работает, при нажатии на кнопку «Вкл.» формируется тестовое событие с кодом **E602**, которое будет передано по каналу, если он будет успешно инициализирован.

Слева от кнопки «Вкл.» отображается количество событий, которые были переданы на пульт с того момента, как канал в последний раз был активен.

5.14.2 Проводные шлейфы

Для каждого проводного шлейфа, который включен на вкладке [Шлейфы](#), отображается его физическое состояние. Например, если шлейф в данный момент в нарушен (в тревоге), то значок, с номером соответствующим номеру шлейфа, будет красным. Если по шлейфу есть неисправность, то это также будет указано в панели состояния. Если шлейф выключен в настройках прибора, то информация по нему отображаться не будет.



Рис. 98: Вкладка «Панель состояния», Шлейфы в состоянии: норма, тревога, короткое замыкание, обрыв

5.14.3 Беспроводные устройства

Для беспроводных устройств в “Панели состояния” отображается следующая информация:

- Оценка качества связи;
- Текущее состояние устройства.



Рис. 99: Вкладка «Панель состояния». вверху - значки беспроводных устройств, внизу - детальная информация

Состояние устройства

На вкладке Беспроводные устройства отображается информация обо всех беспроводных устройствах, записанных в конфигурацию прибора.

Если устройство в тревоге, то весь значок будет окрашен в красный цвет, а при наличии какой-либо неисправности, это будет указано внизу значка. При нажатии на значок беспроводного устройства, можно получить более детальную информацию о его состоянии.

Оценка качества сигнала беспроводных устройств

Беспроводной расширитель, подключенный к прибору, выполняет оценку качества сигнала каждого беспроводного устройства. Индикатором качества связи является кольцо вокруг номера и названия устройства.

Цвет и заполнение кольца соответствует измеренному радиомодулем отношению *сигнал / шум* в сигнале, принятом от беспроводного устройства:

- Отличное - зеленый цвет, кольцо полностью заполнено;
- Хорошее - желтый цвет, кольцо частично заполнено;
- Плохое - красный цвет, кольцо частично заполнено;
- Нет связи - красный цвет, кольцо полностью заполнено.

6 Удалённый доступ к прибору

6.1 Описание технологии удалённого доступа

Удалённый доступ к прибору включает в себя следующие функции:

- Удалённое обновление программного обеспечения на объекте
- Удалённое конфигурирование объекта
- Удалённое взятие и снятие объекта с охраны пользователем
- Удалённое взятие и снятие объекта с охраны оператором пульта
- Управление состоянием дебиторской задолженности

Для работы всех перечисленных функций необходимо совместимое пультовое программное обеспечение, например, «Центр охраны». Дополнительно, для работы функций удалённого обновления «прошивок», конфигурирования и взятия/снятия пользователем, необходимо подключение прибора к «Облаку» (публичному Облаку Си-Норда – `cloud.cnord.net` – или частному Облаку охранной организации).

Схема подключения выглядит следующим образом:

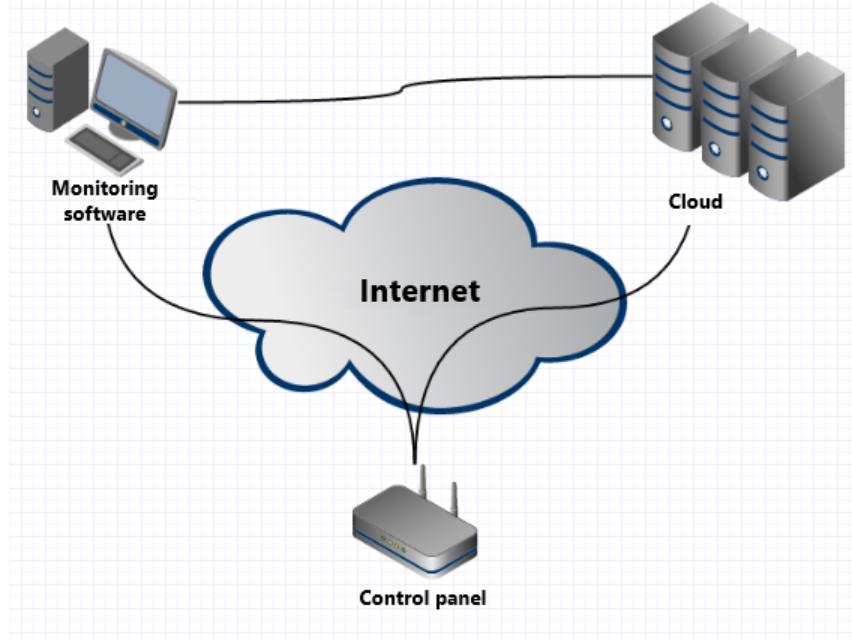


Рис. 100

Прибор подключается и к пультовому ПО, и к «Облаку» по протоколу CML с использованием потокового шифрования (*Протокол CML – C.Nord Markup Language – разработка компании Си-Норд*). Пультовое ПО также подключается к «Облаку» по зашифрованному протоколу.

6.1.1 Канал связи прибор ↔ пульт

Данный канал связи используется для работы охранных функций прибора, таких как:

- Передача событий (тревоги/постановки/снятия/неисправности) на пультовое ПО
- Удалённое взятие и снятие объекта с охраны оператором пульта
- Управление состоянием дебиторской задолженности

В общем случае прибор соединяется с пультом через публичную сеть (Интернет). Однако, некоторые охранные предприятия используют для связи прибор ↔ пульт выделенные внутренние подсети операторов GSM-связи или локальные сети Ethernet.

Для передачи событий на пульт могут использоваться разнообразные каналы связи: Ethernet, GPRS, CSD, Voice, SMS.

Важно: удалённое взятие/снятие и управление дебиторской задолженностью работают только при подключении прибора по IP-каналу связи: Ethernet или GPRS.

6.1.2 Канал связи прибор \longleftrightarrow «Облако»

Данный канал связи используется для работы сервисных функций прибора, таких как:

- Удалённое обновление программного обеспечения на объекте
- Удалённое конфигурирование объекта
- Удалённое взятие и снятие объекта с охраны пользователем

В случае использования публичного «Облака» прибор соединяется с «Облаком» через сеть Интернет. Если же используется «Частное облако», возможна организация подключения через выделенные внутренние подсети операторов GSM-связи или локальные сети Ethernet.

Для работы всех сервисных функций прибор должен находиться на IP-связи с «Облаком» по Ethernet или GPRS.

Важно: возможные перерывы в связи прибор \longleftrightarrow «Облако» никак не влияют на охранные функции прибора.

6.1.3 Канал связи пульт \longleftrightarrow «Облако»

Данный канал связи используется для обеспечения работы сервисных функций прибора.

Пультовое ПО передает в «Облако»:

- информацию об инженерах и их разрешениях
для работы панели инженера
- информацию об администраторах личного кабинета и их объектах
*для работы личного кабинета *my.spord.net* и мобильного приложения MyAlarm*
- события по объектам
для работы личного кабинета и мобильного приложения

«Облако» передает в Пультовое ПО:

- события о попытках подключения инженера к объекту
для работы панели инженера
- события о попытках взятия/снятия из мобильного приложения MyAlarm
для работы мобильного приложения
- события о проверке тревожной кнопки при помощи Call-центра
для работы автоматизированной проверки тревожной кнопки

В случае использования публичного «Облака» пультовое ПО соединяется с «Облаком» через сеть Интернет. Если же используется «Частное облако», возможна организация подключения через локальные сети Ethernet.

Важно: возможные перерывы в связи пульт \longleftrightarrow «Облако» никак не влияют на охранные функции прибора.

6.2 Настройка удалённого доступа

Удалённый доступ к прибору возможен только в случае, если на пульте, к которому подключен прибор, установлено совместимое программное обеспечение, например, «Центр охраны». Чтобы воспользоваться функцией удалённого доступа к прибору, необходимо:

1. Создать инженера в пультовом ПО
2. Выдать инженеру права на удалённый доступ к определенным объектам

6.2.1 Создание инженера

Для того чтобы создать учетную запись для инженера в программном обеспечении «Центр охраны», необходимо запустить модуль «Менеджер персонала» и нажать на кнопку «Создать» на вкладке «Инженеры»:

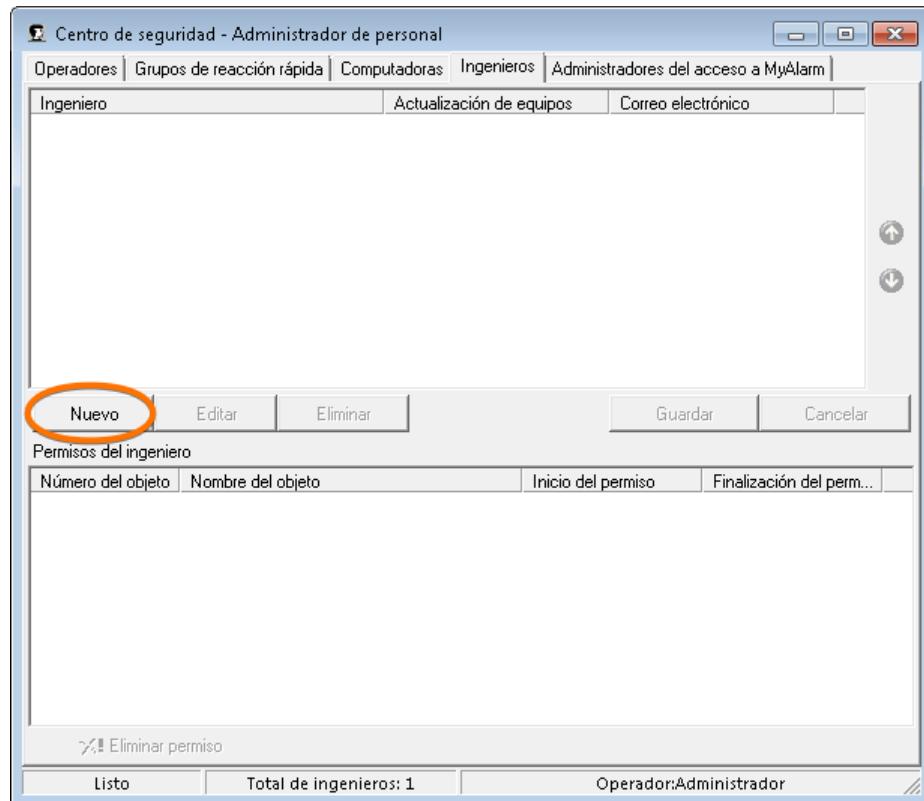


Рис. 101

В открывшемся окне необходимо заполнить все поля с информацией об инженере:



Рис. 102

Особо внимательно следует указывать значение для поля «Электронная почта». Именно на адрес электронной почты, указанный в этом поле, будет отправлено письмо со ссылкой, по которой инженеру необходимо будет перейти для завершения учётной записи в «Облаке». Электронная почта инженера служит для его идентификации в «Облаке». После того как инженер будет создан, изменить значение этого поля нельзя. Если инженер, для которого создается учетная запись, должен иметь возможность удалённо обновлять программное обеспечение на приборах, которые установлены на объектах, необходимо установить галочку «Разрешить инженеру удаленно обновлять программное обеспечение на объектовых приборах». Данная настройка доступна в «Центре охраны» версии 5 и выше.

Важно: разрешение инженера на обновление программного обеспечения распространяется на все объекты охранного предприятия с функцией удалённого обновления «прошивки».

Для того чтобы изменения вступили в силу, нужно на вкладке «Инженеры» нажать на кнопку «Сохранить». После этого информация об инженерах и их праве обновлять приборы синхронизируется с «Облаком».

6.2.2 Выдача разрешений инженеру

Для того чтобы в ПО «Центр охраны» предоставить инженеру разрешение на удалённый доступ к оборудованию, установленному на объекте, необходимо выполнить следующие действия:

1. Запустить модуль «Менеджер объектов»
2. Выбрать объект, к которому необходимо разрешить удалённый доступ
3. Перейти на вкладку «Обслуживание»
4. Нажать на кнопку «Добавить разрешение»

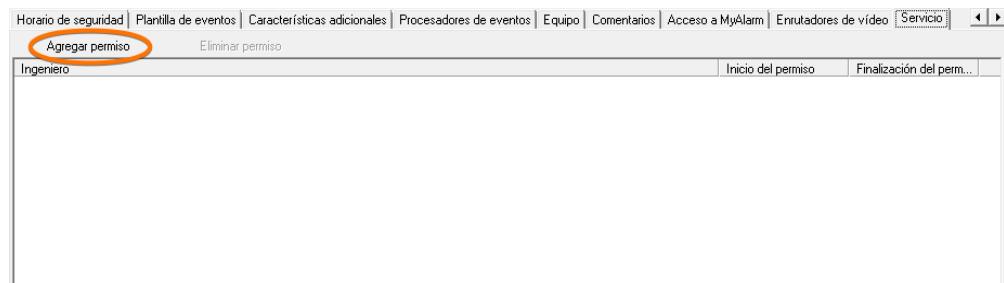


Рис. 103

5. В появившемся окне выбрать инженера, которому необходимо предоставить удалённый доступ к объекту

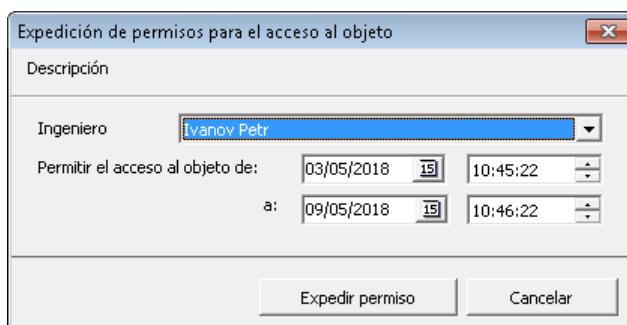


Рис. 104

6. Указать временной интервал, в течение которого будет действовать разрешение.
7. Нажать на кнопку «Выдать разрешение».

6.3 Удалённое конфигурирование устройств

Важно: удалённая настройка доступна только для устройств, которые сконфигурированы для использования IP-каналов связи: Ethernet или GPRS.

Важно: описанные в данном разделе функции работают только, если устройство подключено к программному обеспечению «Центр охраны».

6.3.1 Выбор объекта для конфигурирования

Для удалённого изменения настроек в приборах предназначена вкладка «Удалённый доступ к объектам» в панели инженера:

The screenshot shows a list of objects for configuration:

- Objeto 115, acceso a 14:31 11.05.2018
Nord GSM 5.2, versión 17.17
[Configurar el dispositivo](#)
- Objeto 693, acceso a 14:32 11.05.2018
Nord GSM Mini 13.2, versión 17.18
[Configurar el dispositivo](#)
- Objeto 855, acceso a 14:33 11.05.2018
Nord GSM Air 15.2, versión 17.23
[Configurar el dispositivo](#)
- Objeto 992, acceso a 14:33 11.05.2018
Nord GSM Air 15.2, versión 17.17
[Configurar el dispositivo](#)

© 1992—2018, CNord

Puc. 105

В данной вкладке отображается список объектов, которые доступны инженеру для конфигурирования в данный момент. Перечень и время действия разрешений настраиваются в программном обеспечении «Центр охраны».

Чтобы приступить к настройке, необходимо нажать на соответствующий номер объекта.

6.3.2 Работа с конфигурацией

Открывшееся окно настройки прибора аналогично конфигуратору, предназначенному для настройки прибора, подключенного к компьютеру, который описан в разделе «Конфигурирование»:

The screenshot shows the configuration interface for the Nord GSM 5.2 device, version 17.23. The current object is number 115. The configuration table for zones is as follows:

Zonas	Número	Tipo	Norma	Resistencias	Retraso de entrada	Retraso de salida
Usuarios	1	Activar	De seguridad	Cerrado	no hay	5 minutos
Particiones	2	Activar	24 horas	Cerrado	no hay	
Varios	3	Activar	De seguridad sin sirena	Cerrado	dos	sin
Security center	4	Activar	Botón de pánico sin fijación	Abierto	no hay	
Radio	5	Activar	De seguridad	Cerrado	dos	sin
Operadores GSM	6	Activar	De seguridad	Abierto	dos	sin
Sistemas automáticos	7	Activar	De seguridad	Abierto	dos	sin
Panel de estado	8	Activar	De seguridad	Abierto	dos	sin

© 1992—2018, CNord

Puc. 106

При открытии окна настройки с прибора считывается его текущая конфигурация. Далее можно внести необходимые изменения и записать их на устройство соответствующей кнопкой. После успешной загрузки конфигурации на прибор выведется сообщение: **Настройки сохранены для записи на устройство**.

Важно: считывание и изменение конфигурации доступны только для устройств, которые в данный момент находятся на связи с «Облаком». Если это не так, будет выведено сообщение об ошибке: **Коммуникатор, установленный на объекте, в настоящий момент не подключен к "Облаку". Пожалуйста, попробуйте подключиться к объекту позже.**

Обратите внимание, что некоторые поля конфигурации, к примеру, адреса для подключения к пульту, удалённо изменить нельзя. Это исключает возможность удалённо сломать связь прибора с пультом и с «Облаком». Также недоступны действия, которые требуют локального взаимодействия с прибором на объекте, например, связывание беспроводных датчиков или добавление ТМ-ключей.

6.3.3 Особенности работы

Одновременная работа

Несмотря на то что разрешения на конфигурирование одного объекта могут быть одновременно выданы нескольким инженерам, непосредственную настройку одновременно может осуществлять только один инженер. Доступ остальных инженеров к панели настройки блокируется и при попытке открыть объект для настройки выводится предупреждение: **Объект в настоящий момент уже конфигурируется или обновляется.**

Приоритет локального конфигурирования

Если во время удалённого конфигурирования одним инженером, другой инженер изменит настройки прибора локально при помощи «настольного» конфигуратора, применить удалённые настройки уже станет невозможно – будет выведено сообщение об ошибке загрузки конфигурации.

6.4 Удалённое обновление ПО на устройстве

Важно: удалённое обновление программного обеспечения работает только для устройств, которые сконфигурированы для использования IP-каналов связи: Ethernet или GPRS.

Важно: описанные в данном разделе функции работают только, если устройство подключено к программному обеспечению «Центр охраны».

6.4.1 Информация об объектах на пульте

Для удалённого обновления «прошивок» в приборах предназначена вкладка «Обновление программного обеспечения на объектах» в панели инженера:

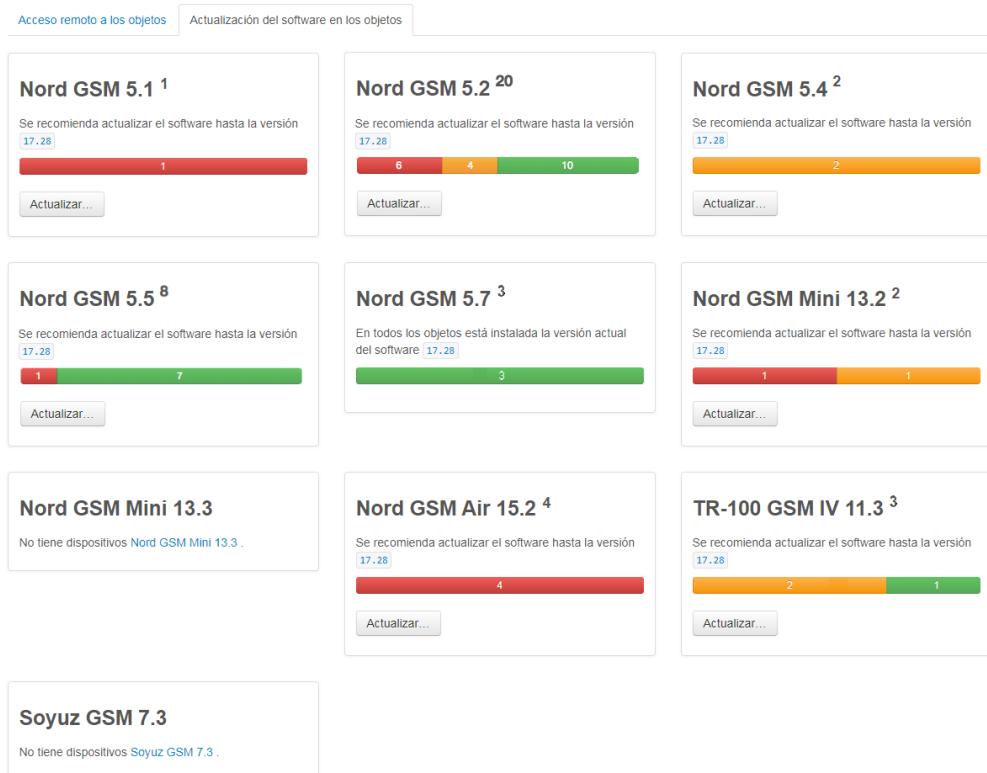


Рис. 107

На данной вкладке отображается статистика по версиям программного обеспечения, сгруппированная по типам приборов. Например, для прибора «Норд GSM»:



Рис. 108

- 20 устройств «Норд GSM» работают на данный пульт
- Актуальная версия ПО для «Норд GSM» – 5.40
- 10 приборов в данный момент работают на старой версии, из них:
 - 6 – обозначены красным – не планируется обновлять
 - 4 – обозначены жёлтым – находятся в процессе обновления
- 10 приборов работают на актуальной версии ПО для данного оборудования

Чтобы открыть страницу обновления ПО на устройствах данного типа, необходимо нажать на кнопку «Обновить...»

6.4.2 Процесс удалённого обновления ПО на устройстве

Процесс обновления программного обеспечения на устройстве состоит из нескольких этапов и спроектирован таким образом, чтобы работать даже в сетях с очень неустойчивым GPRS-сигналом.

Постановка в очередь на обновление

Из панели инженера «Облаку» подаётся команда для постановки устройства в очередь на обновление.

Если устройство находится на связи с «Облаком», то на устройство будет отправлена команда для повторного подключения и инициации процесса обновления.

Если устройство не находится на связи с «Облаком», то процесс обновления не начнётся до тех пор, пока устройство не выйдет на связь.

Загрузка актуальной «прошивки»

Как только устройство получило команду на обновление, оно начинает загрузку архива с актуальной версией программного обеспечения. Полный объем файла составляет от 200 до 500 Кб в зависимости от типа устройства. Загрузка «прошивки» происходит по частям, чтобы сократить влияние обрывов связи.

Длительность этапа загрузки сильно зависит от качества связи и может составлять от нескольких минут на канале Ethernet до нескольких часов на канале GPRS.

Проверка архива

После полной загрузки файла «прошивки» прибор проверяет его целостность и пригодность к использованию на данном типе прибора и на данной аппаратной версии платы. Если все контрольные суммы совпадают и все проверки совместимости пройдены, «прошивка» помечается, как «готова к установке».

Обновление

Далее прибор ожидает состояния, когда хотя бы один из разделов будет снят с охраны, и перезагружается для применения обновления.

Длительность этапа обновления составляет не более 10 секунд.

Включение

После обновления «прошивки» идет обычное включение прибора. Все настройки и состояние охраны для разделов сохраняются в том же состоянии, как были до обновления.

6.4.3 Обновление ПО на выбранном объекте

Если есть необходимость проверить функции новой версии программного обеспечения на одном или нескольких объектах перед массовой установкой, можно воспользоваться обновлением ПО на выбранном объекте.

Для этого на странице обновления ПО нужно нажать на кнопку «Обновить по номеру объекта...»:

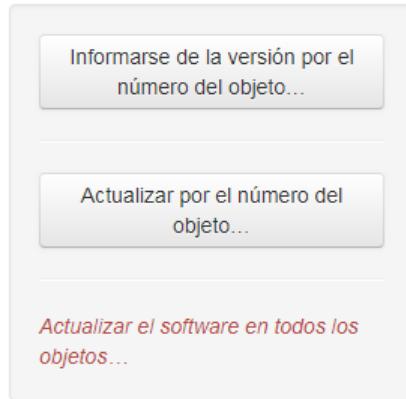


Рис. 109

В появившемся диалоге ввести номер объекта для обновления:

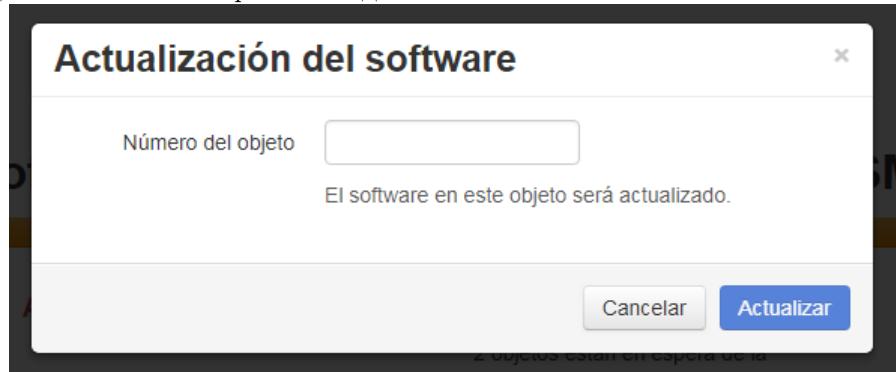


Рис. 110

И нажать кнопку «Обновить». После этого данный объект будет добавлен в очередь на обновление ПО.

6.4.4 Обновление ПО на всех объектах

После проверки ПО на нескольких объектах, можно добавить в очередь на обновление все оставшиеся с предыдущей версией ПО объекты.

Для этого на странице обновления ПО нужно нажать на кнопку «Обновить программное обеспечение на всех объектах...»

В появившемся диалоге:

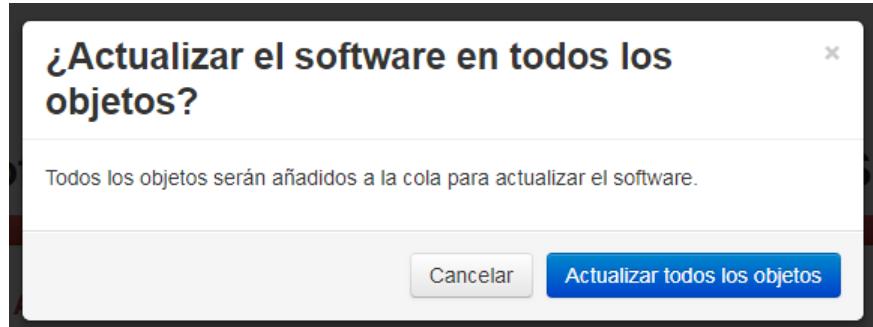


Рис. 111

нажать кнопку «Обновить все объекты». После этого все объекты данного типа с неактуальной версией ПО будут добавлены в очередь на обновление.

6.4.5 Остановка процесса обновления

Если по какой-то причине появилась необходимость остановить процесс обновления, то его можно прервать до тех пор, пока прибор целиком не загрузил файл обновления.

Для этого необходимо нажать «Отменить обновление...» и подтвердить действие.

7 Коды событий

Contact ID	EPAF	Событие	Примечание
E110	SY	Пожар	Пожарная тревога
E118	SY	Предупреждение	Опасность пожара
E120	SX	Тревога	Тревожная кнопка
E121	RP	Тревога	Снятие под принуждением
E130	AA..DR	Тревога	Охранный шлейф
E133	AA..DR	Тревога	24-часовой охранный шлейф
E137	RS	Тревога	Корпус прибора открыт (тампер)
E138	SQ	Предупреждение	Вероятная тревога
E141	AA..DR	Тревога	Обрыв шлейфа, взятого под охрану
E142	AA..DR	Тревога	Короткое замыкание шлейфа, взятого под охрану
E144	AA..DR	Тревога	Корпус датчика открыт (тампер)
E146	AA..DR	Тревога	Охранный шлейф без сирены (тихая тревога)
E150	AA..DR	Тревога	24-часовой не охранный шлейф
E151	AA..DR	Тревога	Утечка газа
E154	AA..DR	Тревога	Протечка воды
E301	RU	Неисправность	Отключение 220 В
E302	RW	Неисправность	АКБ разряжена
E306	–	Система	Настройки прибора изменены
E309	RW	Неисправность	АКБ неисправна
E311	RW	Неисправность	АКБ отключена
E314	HK..LB	Неисправность	Неисправность основной батареи беспроводного устройства или питания пожарного шлейфа, подключенного через ППШ-2
E321	SC	Неисправность	Сирена неисправна
E331	HK..LB	Неисправность	Обрыв шлейфа
E332	HK..LB	Неисправность	Короткое замыкание шлейфа
E381	HK..LB	Неисправность	Связь с беспроводным устройством потеряна
E384	HK..LB	Неисправность	Неисправность резервной батареи беспроводного устройства
E401	QT..23	Снятие	Снятие кодом пользователя
E403	QT..23	Снятие	Автоматическое снятие
E461	SL	Предупреждение	Подбор кода пользователем
E469	–	Снятие	Снятие раздела, который был под охраной, но при конфигурировании был удален из настроек прибора
E470	TA	Отказ от взятия	Вслед за этим сообщением передается причина отказа от взятия (коды E471 – E476)
E471	–	Отказ от взятия	Не оплачены услуги охраны
E472	RU	Отказ от взятия	Отсутствие 220 В

E473	74	Отказ от взятия	Отсутствие IP-связи с пультом охраны
E474	–	Отказ от взятия	Неисправность в шлейфе, который входит в раздел, который берется под охрану
E475	–	Отказ от взятия	Тревога в шлейфе, который входит в раздел, который берется под охрану
E476	RS	Отказ от взятия	Корпус прибора открыт
E499	QT..23	Снятие	Снятие с пульта охраны
E521	–	Система	Сирена выключена в настройках
E601	SM	Тест	Событие формируется при включении канала в панели состояния
E602	SN	Тест	Автотест
E627	–	Система	Включен режим программирования по USB
E628	–	Система	Выключен режим программирования по USB
E750	–	Система	Неверный пароль при подключении по USB
E751	–	Система	Дискретный выход замкнут
E752	–	Система	Запущен сброс значений параметров в заводские
E754	–	Система	Переключение канала по команде системы аудита
E756	56	Неисправность	Неисправность клавиатуры
E757	57	Неисправность	Неисправность связи с БВИ «Пожар»
E758	58	Неисправность	Неисправность связи с «СН-Радио»
R110	DS..HJ	Сброс	Пожарная тревога
R118	DS..HJ	Сброс	Опасность пожара
R120	DS..HJ	Сброс	Тревожная кнопка
R130	DS..HJ	Сброс	Охранный шлейф
R133	DS..HJ	Сброс	24-часовой охранный шлейф
R137	RT	Сброс	Корпус прибора закрыт (тампер)
R141	DS..HJ	Сброс	Норма шлейфа после обрыва (под охраной)
R142	DS..HJ	Сброс	Норма шлейфа после короткого замыкания (под охраной)
R144	DS..HJ	Сброс	Корпус датчика закрыт (тампер)
R146	DS..HJ	Сброс	Охранный шлейф без сирены (тихая тревога)
R150	DS..HJ	Сброс	24-часовой не охранный шлейф
R151	DS..HJ	Сброс	Утечка газа
R154	DS..HJ	Сброс	Протечка воды
R301	RV	Восстановление	220В восстановлены
R302	RX	Восстановление	АКБ заряжена
R305	RR	Система	Перезапуск прибора
R309	RX	Восстановление	АКБ исправна
R311	RX	Восстановление	АКБ подключена
R314	DS..HJ	Восстановление	Основная батарея беспроводного устройства подключена

R321	SD	Восстановление	Сирена исправна
R331	DS..HJ	Восстановление	Норма шлейфа после обрыва
R332	DS..HJ	Восстановление	Норма шлейфа после короткого замыкания
R381	DS..HJ	Восстановление	Связь с беспроводным устройством восстановлена
R384	DS..HJ	Восстановление	Резервная батарея беспроводного устройства подключена
R401	OV..WX	Взятие	Взятие кодом пользователя
R403	PR	Взятие	Автоматическое взятие
R499	OV..WX	Взятие	Взятие с пульта охраны
R521	–	Система	Сирена включена в настройках прибора
R751	–	Система	Дискретный выход разомкнут
R752	–	Система	Отменен сброс значений параметров
R753	–	Система	Перезапуск по неизвестной причине
R754	–	Система	Перезапуск по команде системы аудита
R755	–	Система	Дискретный выход замыкается-размыкается
R756	64	Восстановление	Восстановление неисправности клавиатуры
R757	65	Восстановление	Восстановление связи с БВИ «Пожар»
R758	66	Восстановление	Восстановление связи с «СН-Радио»
R903	–	Система	Прошивка устройства обновлена