

INSTRUKCJA UŻYTKOWNIKA

Rozwiązanie dla małych
instalacji w oparciu
o system JA-10



1. WPROWADZENIE	3
2. OBSŁUGA SYSTEMU JABLOTRON 10	3
2.1 Uwierzytelnianie kodem z klawiatury	5
2.2 Używanie klawiatury systemu	6
2.2.1 Ustawienie alarmu	9
2.2.2 Rozbrajanie alarmu	10
2.2.3 Częściowe uzbrajanie alarmu	10
2.2.4 Rozbrojenie pod przymusem	11
2.2.5 Zakończenie aktywowanego alarmu	11
2.2.6 Sterowanie strefą przez uwierzytelnienie	12
2.2.7 Kontrola strefy za pomocą menu klawiatury	12
2.3 Obsługa centrali alarmowej za pomocą pilota	12
2.4 Obsługa systemu za pomocą komputera i przewodu USB (J-Link)	13
2.5 Obsługa centrali alarmowej za pomocą menu głosowego	14
2.6 Obsługa systemu za pomocą interfejsu sieciowego MyJABLOTRON	14
2.7 Obsługa centrali alarmowej za pomocą aplikacji mobilnej MyJABLOTRON	15
2.8 Obsługa centrali alarmowej za pośrednictwem SMS	15
2.9 Zdalna obsługa systemu za pomocą komputera (J-Link)	16
2.10 Sterowanie wyjściami PG	16
2.10.1 Przyciski funkcji na klawiaturze	16
2.10.2 Uwierzytelnianie z klawiatury użytkownika	17
2.10.3 Zdalne sterowanie	17
2.10.4 Wybór numeru	17
2.10.5 Komunikat SMS	17
3. BLOKOWANIE W SYSTEMIE	17
3.1 Blokowanie użytkowników	17
3.2 Blokowanie czujek	17
3.3 Dezaktywacja kalendarzy	18
4. USTAWIENIA UŻYTKOWNIKA DLA CENTRALI ALARMOWEJ	18
4.1 Zmiana kodu dostępu użytkownika	18
4.2 Zmiana, usuwanie lub dodawanie karty/breloka RFID	18
4.3 Zmiana nazwy użytkownika lub numeru telefonu	18
4.4 Dodawanie/usuwanie użytkownika	18
4.5 Konfiguracja zdarzeń kalendarzowych	19

5. HISTORIA ZDARZEŃ	19
5.1 Za pomocą klawiatury LCD	19
5.2 Korzystanie z programu J-Link i komputera	19
5.3 Logowanie do aplikacji MyJablotron (sieciowej/mobilnej)	19
6. CZYM JEST INTERFEJS SIECIOWY MyJABLOTRON?	19
7. KONSERWACJA OKRESOWA	20
8. SPECYFIKACJA TECHNICZNA	21
9. SŁOWNIK TERMINÓW	22

Dziękujemy za wybór systemu alarmowego JABLOTRON. Niniejsza instrukcja obsługi dotyczy zestawu centrali alarmowej JA-10K oraz klawiatur JA-10E i JA-15E. System ten jest unikalnym rozwiązaniem do ochrony wnętrz i personelu w obiektach komercyjnych i mieszkalnych, oferującym możliwość zastosowania zarówno urządzeń przewodowych, jak i bezprzewodowych. Systemem JABLOTRON 10 niezwykle łatwo sterować. Prostota sterowania polega na zastosowaniu dwuetapowego uwierzytelniania za pomocą kodu lub breloka RFID, po którym następuje naciśnięcie przycisku funkcji na klawiaturze. Przy aktywnym profilu systemu „Domyślny” można zastosować sposób odwrotny. Najpierw należy nacisnąć przycisk funkcji, a następnie dokonać uwierzytelnienia. Systemem alarmowym można również sterować za pomocą samego uwierzytelnienia. Dostęp zdalny za pośrednictwem naszego interfejsu sieciowego oraz aplikacji mobilnej pozwala go obsługiwać z dowolnego miejsca.



System JABLOTRON 10 jest przeznaczony do użytku przez maksymalnie 32 użytkowników i można go podzielić na 4 niezależne strefy. Możliwe jest podłączenie do 32 urządzeń. System oferuje 4 wielofunkcyjne wyjścia programowalne (np. na potrzeby automatyki domowej).

OSTRZEŻENIE:

Instalację i programowanie systemu alarmowego JABLOTRON 10 powinni prowadzić specjaliści. Użytkownik może jedynie zarządzać funkcjami użytkownika i uprawnieniami dostępowymi do systemu alarmowego.

System alarmowy można zaprogramować tak, by wykorzystywał różne sposoby sterowania z możliwością wyboru podczas instalacji w charakterze profili systemu, jak:

- Domyślny Jablotron
- EN 50131, st.2
- INCERT, st.2
- I inne

Niektóre funkcje użytkownika będą ograniczone zależnie od wybranego profilu. Należy poprosić serwisanta o szczegółowy wykaz funkcji.

2. OBSŁUGA SYSTEMU JABLOTRON 10

Systemem alarmowym można sterować za pomocą klawiatury systemu i na kilka innych sposobów. Do rozbrojenia alarmu zawsze konieczne jest uwierzytelnianie w formie identyfikacji użytkownika. System wykrywa tożsamość użytkowników i pozwala im obsługiwać części systemu, do sterowania którymi zostali przypisani. Można wybrać różne sposoby uzbrajania systemu z uwierzytelnianiem lub bez. W przypadku uzbrajania bez uwierzytelnienia, uwierzytelnienie nie jest konieczne, ponieważ system można uzbroić przez naciśnięcie przycisku funkcji na klawiaturze. Centralę alarmową można skonfigurować do sterowania za pośrednictwem samego uwierzytelnienia. Przy każdym dostępie do systemu w pamięci centrali rejestrowane i przechowywane są takie informacje jak nazwa użytkownika, data i godzina. Informacje te są dostępne bez ograniczeń czasowych. Użytkownik może anulować uruchomiony alarm (wyłączyć syreny) na podstawie uwierzytelnienia w dowolnej części systemu (zależnie od posiadanych uprawnień dostępowych). Nie oznacza to jednak automatycznego rozbrojenia systemu (o ile nie zmieniono domyślnego ustawienia systemu).

Uwaga: Zależnie od konfiguracji instalacji i ustawień systemu, niektóre z poniższych opcji mogą nie być dostępne. Konfigurację instalacji należy skonsultować z serwisantem.

OSTRZEŻENIE: system alarmowy monitoruje liczbę nieprawidłowo wpisanych kodów użytkownika oraz wykorzystanie nieprawidłowych kart dostępu. Po 10 nieudanych próbach uwierzytelnienia uruchomi się alarm sabotażu, a centrala alarmowa zostanie czasowo zablokowana, zależnie od konfiguracji systemu alarmowego (wybrany profil systemu).

Użytkownicy i ich uprawnienia dostępne

UWIERZYTELNIANIE KODEM	OPIS TYPU
Kod SMA	Ten kod posiada najwyższy poziom uwierzytelnienia na potrzeby konfiguracji zachowania systemu i jako jedyny służy do odblokowania systemu po aktywacji alarmu. Pozwala wejść w tryb serwisowy, daje dostęp do wszystkich zakładek z opcjami, w tym do komunikacji z SMA, i może uniemożliwić dostęp do niej serwisantowi (kod serwisowy). Dopóki parametr „Usługa ograniczona do administratora / uprawnienia SMA” pozostaje niezaznaczony, kod SMA może sterować wszystkimi strefami i wyjściami PG w systemie. Ten kod pozwala dodawać nowych Administratorów oraz innych użytkowników o niższym poziomie autoryzacji, a także przypisywać im kody, breloki i karty RFID. Pozwala on także na dostęp do kasowania alarmu i pamięci alarmów sabotażowych. Liczbę kodów SMA ogranicza wyłącznie wolne miejsce w centrali alarmowej.
Kod serwisowy (serwis)	Pozwala wejść w tryb serwisowy i konfigurować zachowanie systemu. Umożliwia dostęp do wszystkich zakładek z opcjami, w tym do komunikacji z SMA, jeżeli technik SMA wyższego szczebla nie ograniczy dostępu. Dopóki parametr „Usługa ograniczona do administratora / uprawnienia SMA” pozostaje niezaznaczony, kod serwisowy może sterować wszystkimi strefami i wyjściami PG w systemie. Pozwala utworzyć użytkownika z pozwoleniem SMA, innych serwisantów, Administratorów oraz innych użytkowników o niższym poziomie autoryzacji, a także przypisać im kody dostępu, breloki i karty RFID. Pozwala on także na dostęp do kasowania alarmu i pamięci alarmów sabotażowych. Liczbę kodów serwisowych ogranicza wyłącznie wolne miejsce w centrali alarmowej. Domyślny kod fabryczny to 1010 i nie można go skasować.
Administrator (Główny)	Ten kod zawsze zapewnia pełny dostęp do wszystkich stref i umożliwia sterowanie wszystkimi wyjściami PG. Administrator może utworzyć innego Administratora oraz inne kody o niższym poziomie uwierzytelniania, i przypisać im dostęp do stref, wyjść PG, kody dostępu, chipy i karty RFID. Posiada pozwolenie na kasowanie pamięci alarmów. Może być tylko jeden główny kod Administratora, którego nie można skasować. Kiedy opcja „Usługa ograniczona do administratora/prawo SMA” jest aktywna, kod administratora wymaga uwierzytelnienia, by potwierdzić dostęp. Domyślny kod fabryczny to 1234.
Administrator (Inny)	Ten typ kodu Administratora posiada dostęp do stref zaznaczonych przez Administratora głównego, do których drugi Administrator może dodawać nowych użytkowników o tym samym lub niższym poziomie uwierzytelniania w celu sterowania strefami i wyjściami PG, przypisywać im kody dostępu, breloki i karty RFID. Posiada pozwolenie na kasowanie pamięci alarmów w przypisanych strefach. Kiedy opcja „Usługa ograniczona do administratora / uprawnienia SMA” jest aktywna, kod administratora wymaga uwierzytelnienia, by potwierdzić dostęp. Liczbę kodów Administratora (innego) ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.
Użytkownik	Ten kod umożliwia dostęp do sterowania strefami i PG przydzielonymi przez Administratora. Użytkownicy mogą dodać/usunąć własne breloki RFID i karty dostępu, a także zmienić numery telefonów. Posiada pozwolenie na kasowanie pamięci alarmów w przypisanych strefach. Wybrany użytkownik może posiadać ograniczony czasowo dostęp do wybranych stref. Liczbę kodów Użytkownika ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.
Uzbrój	Ten kod może służyć jedynie do uzbrajania wyznaczonej strefy i do sterowania (WŁ./WYŁ.) wyjściami PG, wymagającymi uwierzytelnienia. Użytkownicy o tym poziomie autoryzacji nie mogą zmieniać własnego kodu ani kasować pamięci alarmów. Liczbę kodów Uzbrajania ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.
Wyłącznie PG	Pozwala użytkownikowi sterować wyjściami programowalnymi wyłącznie na podstawie uwierzytelniania. Dotyczy to zarówno włączania, jak i wyłączania. Użytkownicy o tym poziomie uwierzytelnienia nie mają prawa zmieniać własnych kodów. Liczbę kodów wyłącznie dla PG ogranicza jedynie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.
Alarm napadowy	Ten kod służy jedynie do aktywacji alarmu napadowego. Użytkownik tego kodu nie może go zmieniać ani kasować pamięci alarmów. Liczbę kodów alarmu napadowego ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.
Kod ochrony	Jest to kod przeznaczony dla agencji ochrony. Poziom autoryzacji umożliwia uzbrajanie całego systemu. Kod ochrony może rozbroić cały system wyłącznie podczas alarmu lub po jego zakończeniu, jedynie kiedy pamięć alarmów pozostaje aktywna. Użytkownik tego kodu nie może go zmieniać ani kasować pamięci alarmów. Liczbę kodów ochrony ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.
Kod odblokowania	Ten kod służy do odblokowania systemu po jego zablokowaniu przez alarm. Użytkownik tego kodu nie może sterować centralą alarmową, zmieniać jej kodu ani kasować pamięci alarmów. Liczbę kodów odblokowania ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.

2.1 UWIERZYTELNIANIE KODEM Z Klawiatury

Uwierzytelnianie kodem użytkownika wymaga wpisania prawidłowego kodu na klawiaturze lub użycia breloka RFID. W systemie można używać kodów 4 lub 6-cyfrowych (zależnie od wybranego profilu).

CCCC

Znaczenie:

CCCC to kod 4 lub 6-cyfrowy. Dozwolone kody... od 0000 do 9999 (000000 do 999999)

Domyślny kod centrali alarmowej

Administrator: 1234; 123456;

OSTRZEŻENIE: Zaleca się zmianę kodu Administratora podczas pierwszego włączenia zasilania systemu alarmowego.

Bezpieczeństwo kodów dostępu i zbliżeniowych czipów RFID:

Centrala alarmowa pozwala przypisać użytkownikowi jeden kod 4- lub 6-cyfrowy oraz jeden czip RFID na potrzeby uwierzytelniania w systemie. Uwierzytelnianie użytkownika jest niezbędne każdorazowo podczas obsługi systemu za pomocą klawiatury, menu głosowego, aplikacji sieciowych lub mobilnych. Długość kodu wpływa na możliwe kombinacje, a tym samym bezpieczeństwo kodu.

Liczba kombinacji kodu zależy od konfiguracji:

PARAMETRY CENTRALI ALARMOWEJ	4 CYFRY	6 CYFR
„Rozbrojenie pod przymusem” wyłączone, „Uwierzytelnianie standardowe” włączone	$= 10^4 - (\text{Liczba użytkowników} - 1)$	$= 10^6 - (\text{Liczba użytkowników} - 1)$
„Rozbrojenie pod przymusem” włączone, „Uwierzytelnianie standardowe” włączone	$\leq 10^4$ $- ((\text{Liczba użytkowników} - 1) * 3)$	$\leq 10^6$ $- ((\text{Liczba użytkowników} - 1) * 3)$
„Rozbrojenie pod przymusem” wyłączone, „Uwierzytelnianie podwójne” włączone	$= 10^8 * (10^4$ $- (\text{Liczba użytkowników} - 1))$	$= 10^8 * (10^6$ $- (\text{Liczba użytkowników} - 1))$
„Rozbrojenie pod przymusem” włączone, „Uwierzytelnianie podwójne” włączone	$\leq 10^8 * (10^4$ $- ((\text{Liczba użytkowników} - 1) * 3))$	$\leq 10^8 * (10^6$ $- ((\text{Liczba użytkowników} - 1) * 3))$
Używanie tylko karty RFID bez kodu dostępu	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$

Sposoby zwiększenia poziomu ochrony przed niepożądanym odgadnięciem prawidłowego kodu:

- Używanie kodu z większą liczbą cyfr (kody 6-cyfrowe)
- Bardziej zaawansowane rodzaje uwierzytelniania, jak „Uwierzytelnianie podwójne”.

Bezpieczeństwo zdalnego sterowania:

Centrala alarmowa może korzystać z pilotów. Bezpieczeństwo takiego sposobu sterowania zapewnia ponad 1 000 000 kombinacji kodów identyfikacyjnych i specjalna transmisja kodów dynamicznych.

Sposoby obsługi centrali alarmowej JA-100K:**Lokalnie:**

- Klawiatura systemu
- Pilot systemu
- Za pośrednictwem komputera z przewodem USB i oprogramowaniem J-Link

Zdalnie:

- Mobilna aplikacja MyJABLOTRON
- Za pośrednictwem komputera i interfejsu sieciowego MyJABLOTRON
- Telefon komórkowy — za pomocą SMS
- Telefon — korzystając z menu głosowego
- Komputer — za pośrednictwem internetu i oprogramowania J-Link
- Wybór numeru z uwierzytelnionego numeru telefonu (wyłącznie do obsługi wyjść programowalnych).

OSTRZEŻENIE: Zdalne sterowanie może być ograniczone zależnie od zakresu bezpieczeństwa i wybranego profilu Systemu.

2.2 KLAWIATURA SYSTEMOWA



Systemem JABLOTRON 10 można sterować za pośrednictwem klawiatur systemu, które umożliwiają nie tylko sterowanie, ale także wyświetlanie stanów poszczególnych stref. Stany poszczególnych stref wskazują kontrolki stanu A, B, C i D nad wyświetlaczem LCD oraz przyciski funkcji. Centralę alarmową można obsługiwać bezpośrednio (uzbrajanie lub rozbrajanie alarmu i innych funkcji automatyki) za pomocą przycisków funkcji na klawiaturze. Przyciski funkcji i kontrolki stanu podświetlają się na kolorowo, aby wyraźnie zasygnalizować stany stref.



ZIELONA – Rozbrojona



ŻÓŁTA – Częściowo rozbrojona



CZERWONA – Uzbrojona

Upoważnienie

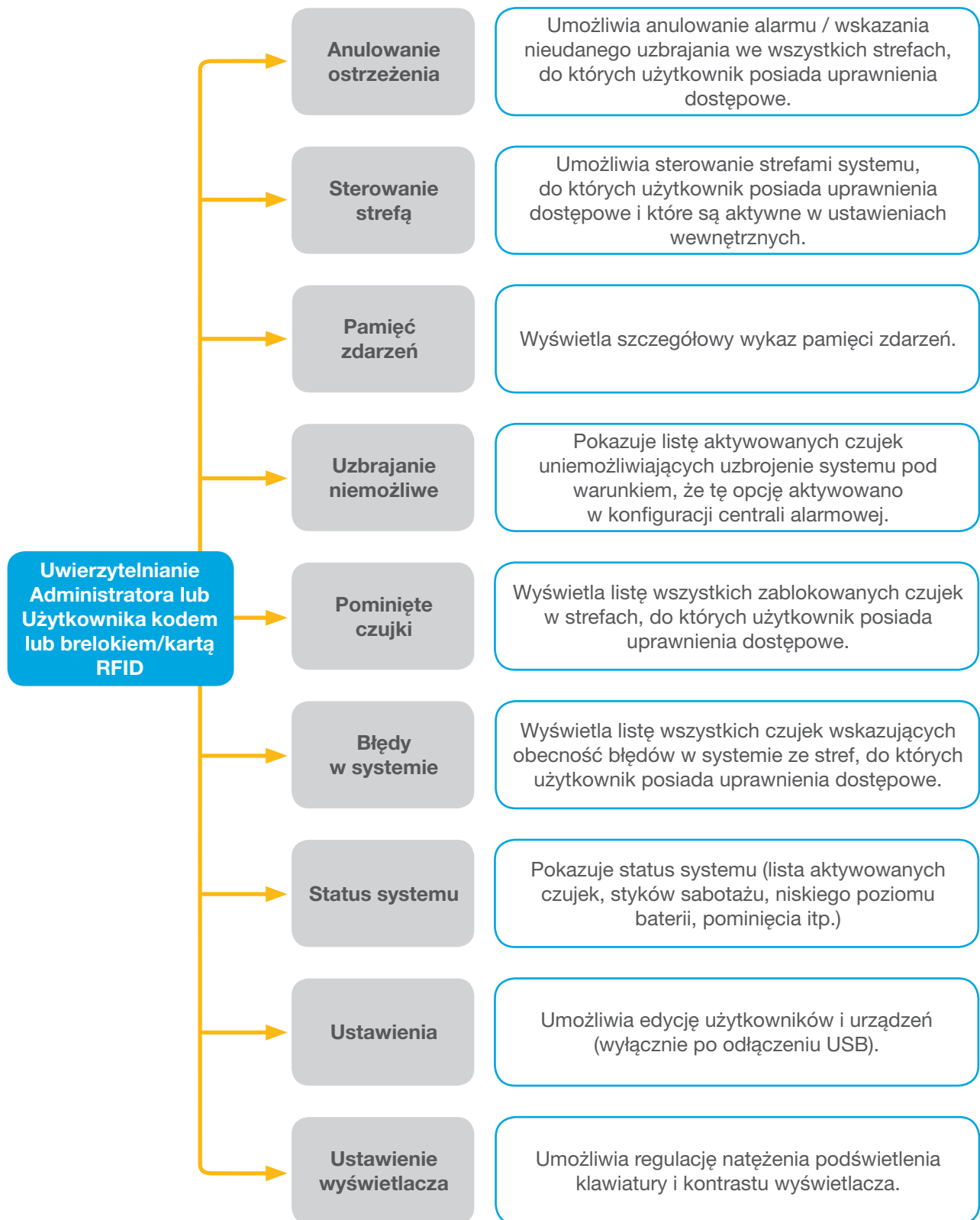
W celu uwierzytelnienia można wpisać kod dostępu na klawiaturze lub skorzystać z karty/breloka RFID przypisanego do danego użytkownika. Każdy użytkownik może posiadać jeden kod i jeden czip RFID (kartę lub brelok).



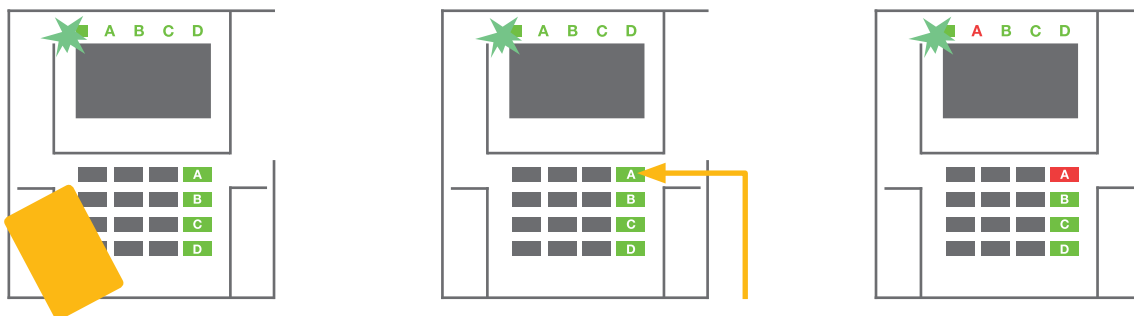
Centrala alarmowa obsługuje czipy RFID kompatybilne z technologią 125 kHz EM Unique. Jeżeli konieczne jest wyższe bezpieczeństwo, system alarmowy można skonfigurować tak, by korzystać z Uwierzytelniania podwójnego za pomocą czipów RFID i kodów (funkcja opcjonalna).

Jeżeli użytkownik pragnie jednocześnie sterować kilkoma strefami, musi dokonać uwierzytelnienia i kolejno nacisnąć przyciski funkcji poszczególnych stref. W ten sposób użytkownik może rozbroić wszystkie strefy (na przykład dom i garaż) w ramach jednego uwierzytelnienia.

Struktura i opis wewnętrznego menu klawiatury na wyświetlaczu LCD



2.2.1 USTAWIENIE ALARMU



1. Należy dokonać uwierzytelnienia za pomocą klawiatury. Zaświecą się przyciski funkcji A, B, C i D dla stref, którymi dany użytkownik może sterować, a kontrolka systemu zacznie migać na zielono.

2. Należy nacisnąć przycisk funkcji, aby uzbroić daną strefę. Kolejno można uzbroić większą liczbę stref. Opóźnienie między zaznaczeniem stref nie może przekraczać 2 sekund.

3. Polecenie zostanie zrealizowane, a klawiatura dźwiękiem powiadomi o czasie na wyjście. Strefa jest teraz uzbrojona, jedynie czujki z reakcją „Alarm opóźniony” zapewnią czas na opuszczenie chronionej strefy podczas czasu na wyjście. Kontrolka stanu i przycisk funkcji dla uzbrojonej strefy zmieni kolor na czerwony.

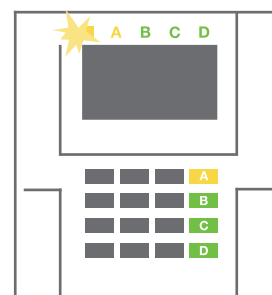
Jeżeli podczas uzbrajania alarmu aktywuje się jakakolwiek czujka (np. otwarte okno), system zareaguje (na podstawie konfiguracji systemu) w jeden z poniższych sposobów:

- Centrala alarmowa uzbroi się samoczynnie. Uruchomione czujki zostaną automatycznie zablokowane.*)
- System zasygnalizuje uruchomione czujki miganiem przycisku funkcji na czerwono przez 8 sekund, a po zakończeniu tego czasu centrala alarmowa zostanie uzbrojona automatycznie (uruchomione czujki zostaną zablokowane). *)
- Strefę z aktywowanymi czujkami można uzbroić także przez wielokrotne naciśnięcie przycisku funkcji. Użytkownik musi potwierdzić zamiar uzbrajania strefy z aktywną czujką (np. otwarte okno). W przeciwnym razie nie dojdzie do uzbrojenia systemu.
- Aktywowana czujka uniemożliwi uzbrajanie strefy. Ten stan wskaże migający na czerwono przycisk funkcji. Czujka uniemożliwiająca uzbrojenie zostanie pokazana na menu wyświetlacza LCD.

***) OSTRZEŻENIE:** Opcja a) i b) nie wynika z normy EN 50131, st.2 (wybrany profil systemu centrali alarmowej)

Jeżeli podczas czasu na wyjście aktywuje się czujka z reakcją „Alarm nagły w strefie” lub po zakończeniu czasu na wyjście pozostanie aktywna czujka z reakcją „Alarm opóźniony w strefie”, dojdzie do ponownego rozbrojenia centrali alarmowej. Nieudane uzbrojenie sygnalizuje kontrolka systemu migająca na żółto. Zostaje ono zgłoszone do SMA i sygnalizuje je syrena zewnętrzna (dotyczy klasy bezpieczeństwa 2).

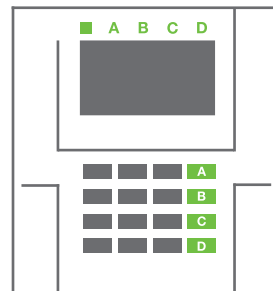
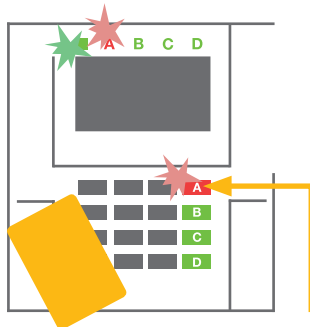
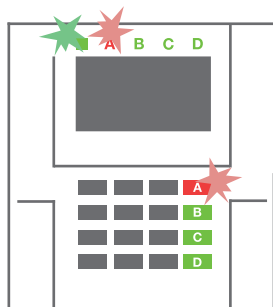
W przypadku konfiguracji centrali alarmowej do uzbrajania bez uwierzytelnienia, uwierzytelnianie nie jest konieczne. Należy nacisnąć przycisk funkcji danej strefy. Można także skonfigurować centralę alarmową na potrzeby uzbrajania za pomocą samego uwierzytelniania.



OSTRZEŻENIE: Uzbrajanie bez uwierzytelniania automatycznie obniża maksymalny poziom bezpieczeństwa do klasy 1. Należy rozważyć wszystkie ewentualne zagrożenia związane z używaniem tej funkcji.

Aby zaprogramować żądane zachowanie systemu alarmowego, należy skonsultować instalację z instalatorem/projektantem systemu.

2.2.2 ROZBRAJANIE ALARMU



1. **Po wejściu do budynku** (aktywacja czujki o reakcji „Alarm opóźniony w strefie”) system zacznie wskazywać czas na wejście dźwiękiem ciągłym i migającą na czerwono kontrolką systemu oraz przyciskiem funkcji dla strefy, w której aktywowano czas na wejście.

2. **Należy dokonać uwierzytelnienia** za pomocą klawiatury — kontrolka systemu zacznie migać na zielono.
3. **Należy nacisnąć przyciski** funkcji dla stref przewidzianych do rozbrojenia.

4. **Trwa realizacja polecenia.** Przyciski funkcji i kontrolka systemu zmieniają kolor na zielony, wskazując strefy rozbrojone.

Uwaga: Przy aktywnym parametrze „Rozbrój strefę przez uwierzytelnianie tylko w czasie na wejście”, samo uwierzytelnianie pozwoli rozbroić strefę, w której aktywowano czas na wejście. W przypadku wielu stref tej opcji należy używać z rozwagą.

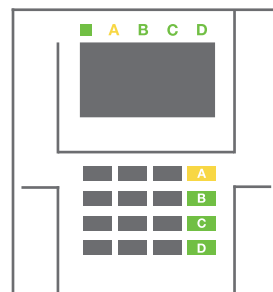
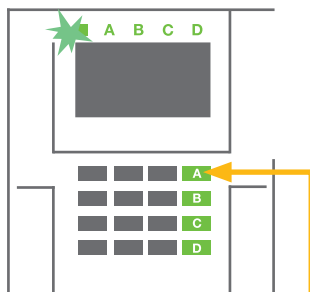
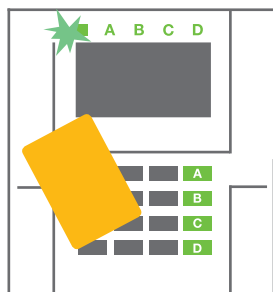
Aby zaprogramować żądane zachowanie systemu, należy skonsultować instalację z instalatorem.

2.2.3 CZĘŚCIOWE UZBRAJANIE ALARMU

OSTRZEŻENIE: Jest to dodatkowa funkcja systemu alarmowego.

System można również skonfigurować tak, by umożliwić jego częściowe uzbrojenie, zapewniające ochronę wyłącznie za pomocą wybranych czujek w danej strefie.

Przykład: W godzinach nocnych można uzbroić wyłącznie czujki drzwi i okien, zaś wybrane czujki ruchu nie będą aktywować alarmu w przypadku stwierdzenia ruchu w obrębie strefy.



1. **Należy dokonać uwierzytelnienia za pomocą klawiatury** (wpisać kod lub zbliżyć kartę lub brelok RFID do czytnika). Przycisk kontrolki systemu zacznie migać na zielono.

2. **Nacisnąć przycisk funkcji** dla wybranej strefy.

3. **Polecenie zostanie zrealizowane**, a przycisk funkcji zacznie świecić żółtym światłem ciągłym, by wskazać częściowe uzbrojenie strefy.

Aby uzbroić cały obiekt, w którym aktywowano uzbrojenie częściowe, należy przez 2 sekundy przytrzymać przycisk do uzbrajania centrali alarmowej lub dwukrotnie go nacisnąć. Po jednokrotnym naciśnięciu przycisk świeci ciągłym żółtym światłem, po naciśnięciu po raz drugi świeci ciągłym czerwonym światłem.

Jeżeli system został już wcześniej częściowo uzbrojony, co wskazuje ciągle żółte światło przycisku funkcji, całość systemu można uzbroić całkowicie przez uwierzytelnienie i naciśnięcie i przytrzymanie żółtego przycisku. Po naciśnięciu przycisku system będzie całkowicie uzbrojony, a przycisk zmieni kolor na czerwony.

Uzbrojenie częściowe można skonfigurować tak, by uwierzytelnianie nie było konieczne.

Aby rozbroić częściowo uzbrojoną centralę alarmową, należy nacisnąć żółty przycisk. Centrala alarmowa zostanie rozbrojona, a przycisk zmieni kolor na zielony.

2.2.4 ROZBROJENIE POD PRZYMUSEM

Umożliwia rozbrajanie centrali alarmowej w specjalnym trybie. System pozornie się rozbraja, ale uruchamia cichy alarm napadowy, który zostaje przekazany wybranym użytkownikom (w tym do SMA).

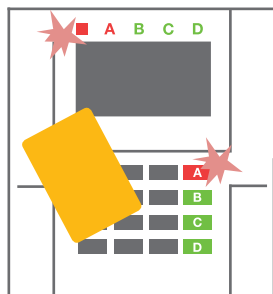
Rozbrajanie w razie napadu realizuje się przez dodanie 1 do ostatniej cyfry obowiązującego kodu. Jeżeli chcą Państwo korzystać z tej funkcji, należy skontaktować się z serwisantem.

Przykład:

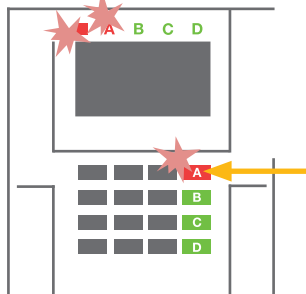
Prawidłowy kod: 9999

Kod do rozbrajania w razie napadu: 9990

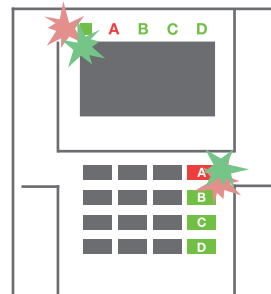
2.2.5 ZAKOŃCZENIE AKTYWOWANEGO ALARMU



1. Należy dokonać uwierzytelnienia za pomocą klawiatury (wpisać kod lub zbliżyć brelok do czytnika).



2. Nacisnąć przycisk funkcji w strefie, w której aktywowano alarm.



3. Rozbrajanie zostanie ukończone, a syreny ucichną. Migające z dużą częstotliwością naprzemienne (zielone/czerwone) światło przycisków funkcji i kontrolki stanu sygnalizują pamięć alarmów.

Trwający aktywny alarm sygnalizuje kontrolka stanu i przycisk funkcji, które migają na czerwono z dużą częstotliwością. Aby zakończyć alarm, należy dokonać uwierzytelnienia za pomocą klawiatury. Strefa pozostaje uzbrojona, przycisk funkcji migający z dużą częstotliwością na czerwono wskazuje pamięć alarmów. Kontrolka będzie migać również po rozbrojeniu systemu.

OSTRZEŻENIE: Jeżeli sygnalizacja pamięci alarmów uruchomiła się pod Państwa nieobecność, należy ostrożnie wejść do budynku, przeszukać historię zdarzeń pod kątem przyczyny alarmu i zachować ostrożność podczas sprawdzania obiektu lub zaczekać na przyjazd agencji ochrony (pod warunkiem że system jest połączony z Centrum Odbioru Alarmów).

Sygnalizacja pamięci alarmów segmentu pozostanie aktywna do czasu ponownego uzbrojenia systemu. Można ją ewentualnie anulować z menu klawiatury. **Menu główne — Anulowanie ostrzeżenia.**

Wskazanie uruchomionego **alarmu sabotażowego** może zostać anulowane wyłącznie przez upoważnionego technika lub administratora.

Uwaga: Korzystając z profilu systemu „Domyślny”, można najpierw wybrać konkretną czynność za pomocą przycisku funkcji, a następnie potwierdzić ją uwierzytelnieniem za pomocą klawiatury.

Zakończenie alarmu pilotem również rozbroi daną strefę.

2.2.6 STEROWANIE STREFĄ PRZEZ UWIERZYTELNIENIE

Serwisant może skonfigurować centralę alarmową tak, by można nią sterować za pomocą samego uwierzytelnienia. W ten sposób można zmienić stan wszystkich stref za pomocą uwierzytelnienia na klawiaturze (wpisując kod dostępu lub korzystając z czipa RFID).

2.2.7 KONTROLA STREFY ZA POMOCĄ MENU KŁAWIATURY

Sterowanie z menu klawiatury:

- Należy dokonać uwierzytelnienia za pomocą prawidłowego kodu lub czipa RFID
- Wejść do menu przez naciśnięcie **ENTER**
- Kontrola strefy → **ENTER**
- Strzałkami wybrać żądaną strefę.
- Wielokrotne naciśnięcie klawisza **ENTER** umożliwi przejście pomiędzy statusami strefy (częściowo uzbrojona / uzbrojona / rozbrojona).

Częściowe uzbrojenie:

1

Pełne uzbrojenie:

1

- Naciśnięcie ESC i opuścić menu.



2.3 OBSŁUGA CENTRALI ALARMOWEJ ZA POMOCĄ PILOTA

Piloty w centrali alarmowej przypisuje instalator. Aby sterować systemem alarmowym, piloty należy przypisać do konkretnych użytkowników, co umożliwi ich identyfikację i zapobiegnie wysyłaniu powiadomień SMS do użytkownika, który w danej chwili obsługuje centralę alarmową (jeżeli w ten sposób skonfigurowano parametry powiadomień). Piloty kontrolują i wskazują stan baterii, posiadają sygnalizację świetlną i dźwiękową.



Piloty

Piloty wysyłają sygnał po każdym naciśnięciu przycisku bez otrzymania informacji zwrotnej z centrali alarmowej. Wysłanie sygnału potwierdzi jedynie krótkie mignięcie czerwonej diody lub sygnał dźwiękowy. Występują w wersji 2 oraz 4 przyciskowej.

Niski poziom energii baterii wskaże czerwona dioda i sygnał dźwiękowy (3 szybkie piknięcia).

W zależności od potrzeb danej instalacji pojedynczy pilot może mieć zadane kilka funkcji. Przykładowo para górnych przycisków służy do uzbrojenia i rozbrojenia strefy alarmowej. Para dolnych przycisków służy do sterowania automatyką budynkową - otwarcie bramy i załączenie lamp.



2.4 OBSŁUGA SYSTEMU ZA POMOCĄ KOMPUTERA I PRZEWODU USB (J-LINK)

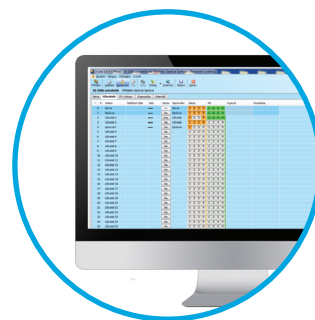
System JABLOTRON 10 można obsługiwać lokalnie lub zdalnie (patrz rozdział 2.9) za pomocą komputera i zainstalowanego oprogramowania J-Link, które można wykorzystać do zarządzania użytkownikami (dodawanie/usuwanie użytkowników, zmiana ich poziomu autoryzacji, numerów telefonu, kodów, kart/breloków itp.).

Oprogramowanie J-link służy do lokalnego łączenia z centralą alarmową. Znajduje się w pamięci systemu alarmowego (FLEXI_CFG/j-link), który pojawi się po połączeniu centrali alarmowej z komputerem za pośrednictwem USB.

System można uzbroić/rozbroić za pomocą ikon na dolnej belce programu lub przycisków „Stan” w zakładce „Strefa”.

OSTRZEŻENIE: System sterowany za pośrednictwem komputera podczas uzbrajania nie sprawdza statusu aktywowanych urządzeń. Może to spowodować uzbrojenie z aktywowanym urządzeniem. Należy zachować ostrożność podczas sterowania systemem w taki sposób!

OSTRZEŻENIE: Oprogramowanie J-Link jest dostępne wyłącznie w wersji dla systemu operacyjnego Windows.



2.5 OBSŁUGA CENTRALI ALARMOWEJ ZA POMOCĄ MENU GŁOSOWEGO

Jeżeli centrala alarmowa posiada zainstalowany komunikator GSM lub PSTN, systemem można sterować za pomocą telefonu komórkowego lub stacjonarnego za pośrednictwem prostego menu głosowego, które w wybranym języku prowadzi użytkownika przez różne opcje. Aby uzyskać dostęp do menu głosowego, należy po prostu wybrać numer telefonu centrali alarmowej.



Dostęp do menu głosowego można aktywować dla wszystkich numerów telefonu bez ograniczeń albo wyłącznie dla autoryzowanych numerów telefonu zapisanych w centrali alarmowej. Zależnie od konfiguracji konieczne będzie uwierzytelnianie przez wpisanie prawidłowego kodu na klawiaturze telefonu. Kiedy użytkownik wejdzie do menu, system przekaże informacje o aktualnym statusie wszystkich stref przypisanych użytkownikowi. Osoba dzwoniąca może wówczas sterować tymi strefami indywidualnie lub zbiorowo za pomocą klawiatury i dostępnych opcji menu.

OSTRZEŻENIE: Należy zachować ostrożność podczas korzystania z tej funkcji. Zdalne uzbrajanie i rozbrajanie może spowodować niepożądane alarmy lub uniemożliwić uzbrojenie w przypadku obecności osób w budynku.

System domyślnie odbiera połączenia przychodzące po trzech tonach (około 15 sekund).

2.6 OBSŁUGA SYSTEMU ZA POMOCĄ PRZEGLĄDARKI INTERNETOWEJ

System JABLOTRON 10 można obsługiwać w sposób prosty i wygodny za pomocą komputera z dostępem do internetu za pośrednictwem interfejsu sieciowego MyJABLOTRON, dostępnego na stronie www.myjablotron.com. Więcej informacji na temat tego interfejsu sieciowego znajduje się w rozdziale 6 poniżej.



MyJABLOTRON — wersja PROFI

Zależnie od kraju lub regionu konto sieciowe w aplikacji MyJABLOTRON może założyć autoryzowany partner JABLOTRON. Loginem jest adres e-mail użytkownika. Na ten adres zostanie wysłane hasło do pierwszego logowania. Hasło można w dowolnej chwili zmienić w ustawieniach użytkownika.

Po zalogowaniu na konto aplikacja MyJABLOTRON pokaże wszystkie aktywne urządzenia, które można monitorować i którymi można sterować.

Menu „Widok” obejmuje zakładkę „Strefy” i „wyjścia PG”. Zależnie od rodzaju zastosowanych czujek, menu może także zawierać takie zakładki jak „Termometry”, „Czujka z kamerą” lub „Liczniki elektryczne”.

Zakładki

- **Strefy** — pozwala wyświetlić i obsługiwać wszystkie strefy w systemie po kliknięciu w symbol zablokowania. Przy pierwszym żądaniu sterowania systemem zostaną państwo poproszeni o wpisanie kodu uwierzytelniania. Późniejsze czynności nie wymagają powtórnego uwierzytelniania do czasu wylogowania.
- **Wyjścia PG** — umożliwia podgląd wszystkich programowalnych wyjść w systemie i sterowanie nimi.
- **Termometry** — pozwala wyświetlić aktualną temperaturę ze wszystkich zainstalowanych termometrów. Pokazuje historię oraz wykresy zmian temperatury w czasie.
- **Czujka z kamerą** — pozwala robić zdjęcia za pomocą wszystkich zainstalowanych czujek ruchu z kamerą lub przeglądać zdjęcia wykonane wcześniej za pomocą tych czujek (galeria zdjęć).

Na dole strony głównej znajduje się wykaz ostatnich zdarzeń w systemie.

MyJABLOTRON oferuje darmowe powiadomienia (za pośrednictwem wiadomości SMS, poczty elektronicznej lub powiadomień PUSH) dla wybranych zdarzeń w strefach systemu, wyjść programowalnych, termometrów lub liczników. Te powiadomienia można ustawić w menu „Ustawienia”.

Każdy system może posiadać tylko jednego użytkownika głównego z uprawnieniami Administratora (właściciela). Ten użytkownik ma prawo udostępnić cały budynek lub jego wybrane strefy, wyjścia PG, czujki z kamerą, termometry i inne urządzenia, innym użytkownikom, których konta MyJABLOTRON zostaną utworzone automatycznie po konfiguracji udostępnienia systemu. Jeżeli użytkownik posiada już konto w aplikacji MyJABLOTRON, udostępniana instalacja pojawi się na pulpicie użytkownika jako kolejne aktywne urządzenie. Powiadomienie o dzielonym dostępie, wraz z hasłem, zostanie wysłane na adres e-mail (login) nowego użytkownika.

MyJABLOTRON – wersja LITE

Zależnie od kraju (lub regionu) klienci mogą być w stanie utworzyć konto i/lub usługi w wersji LITE aplikacji sieciowej MyJABLOTRON.

Usługa LITE posiada ograniczoną funkcjonalność i minimalizuje zapotrzebowanie na transfer danych. Usługa LITE opiera się na wersji usługi PROFi zmodyfikowanej w następujący sposób:

Wersja LITE w porównaniu z wersją PROFi:

- Nie utrzymuje ciągłego połączenia z centralą alarmową
- Ustanowienie połączenia trwa około 1 minutę
- Aktualny status wyświetla się po udanym połączeniu
- Sterowanie systemem (strefy i wyjścia PG) jest możliwe po udanym połączeniu
- Historia zdarzeń nie jest dostępna
- System nie wysyła powiadomień o zdarzeniach (SMS, e-mail, powiadomienia PUSH)
- Galeria zdjęć i robienie zdjęć na żądanie za pomocą czujek z kamerą są niedostępne
- Nie wyświetlają się termometry, liczniki energii elektrycznej i inne obsługiwane urządzenia automatyki (wyjścia PG)

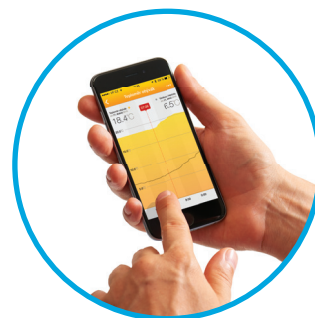
Hasło, będące także loginem, zostanie wysłane na adres e-mail użytkownika. Hasło można w dowolnej chwili zmienić w ustawieniach.

Po zalogowaniu na konto system pokazuje wszystkie aktywne urządzenia, którymi można sterować lub które można monitorować zależnie od wersji aplikacji MyJABLOTRON używanej do ich rejestracji (PROFi lub LITE).

2.7 OBSŁUGA CENTRALI ALARMOWEJ ZA POMOCĄ APLIKACJI MOBILNEJ MyJABLOTRON

Utworzenie konta użytkownika w interfejsie sieciowym MyJABLOTRON (patrz poprzedni rozdział) umożliwia monitorowanie systemu alarmowego i sterowanie nim zdalnie za pomocą aplikacji mobilnej MyJABLOTRON na urządzeniu z systemem Android (wersja 4.0.3 lub nowsza), iPhone (wer. 7 lub nowsza). Aplikację można pobrać bezpłatnie po zalogowaniu na stronie MyJABLOTRON lub z Google Play, AppStore, itp.

Nazwy użytkowników i dane do logowania w aplikacji mobilnej MyJABLOTRON są takie same jak dane do logowania w interfejsie sieciowym MyJABLOTRON.



2.8 OBSŁUGA CENTRALI ALARMOWEJ ZA POŚREDNICTWEM SMS

Jeżeli w centrali alarmowej zainstalowano moduł GSM, można używać poleceń SMS do sterowania poszczególnymi strefami i wyjściami programowalnymi tak samo, jak za pomocą przycisków funkcji na klawiaturze. Wiadomość tekstowa do obsługi systemu ma postać następującą: KOD_KOMENDA. Faktyczne komendy są wstępnie

zdefiniowane (UZBRÓJ/ROZBRÓJ – SET/UNSET). Należy dodać do nich parametr numeryczny wskazujący konkretną strefę.

Jedna wiadomość SMS może sterować jednocześnie wieloma strefami. W takim przypadku numery dodane do polecenia określają strefy.

Przykładowa komenda SMS do uzbrajania stref 2 i 4.

Podkreślenie „_” oznacza odstęp między słowami.

KOD_UZBRÓJ_2_4 / KOD_SET_2_4

Polecenia do sterowania wyjściami programowalnymi może zaprogramować serwisant. Można na przykład ustawić ROLETY W DÓŁ jako polecenie do zamykania rolet na oknach. Można także skonfigurować system tak, by nie wymagał kodu przed poleceniem. W takim przypadku polecenie zostaje zidentyfikowane automatycznie, kiedy system rozpozna numer telefonu użytkownika, z którego wysłano wiadomość SMS.

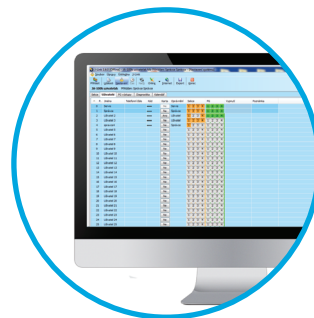
OSTRZEŻENIE: Należy zachować ostrożność podczas korzystania z tej funkcji. Zdalne uzbrajanie i rozbrajanie może spowodować niepożądane alarmy lub uniemożliwić uzbrojenie w przypadku obecności osób w budynku.



2.9 ZDALNA OBSŁUGA SYSTEMU ZA POMOCĄ KOMPUTERA (N-LINK)

System JABLOTRON 10 można obsługiwać zdalnie i lokalnie (patrz rozdział 2.3). W tym celu należy na komputerze zainstalować oprogramowanie N-Link, które może również zarządzać użytkownikami (zmiana kodów, kart/breloków i numerów telefonu).

Aby obsługiwać system zdalnie, należy pobrać program z zakładki „Do pobrania” na stronie www.jablotron.com. Można go znaleźć także na karcie SD centrali alarmowej. Przy pierwszym zdalnym połączeniu z systemem wymagany jest kod rejestracji do systemu bezpieczeństwa (kod 14-cyfrowy) i numer telefonu karty SIM (jeżeli jest używana). Dostęp zdalny rozpoczyna się przez kliknięcie przycisku „Internet” w menu głównym.



Po ustanowieniu połączenia centralą alarmową można sterować tak samo, jak w przypadku połączenia za pomocą przewodu USB (patrz rozdział 2.4).

System można uzbroić/rozbroić za pomocą ikon stref na dolnej belce programu lub przycisków „Stan” w zakładce „Strefa”.

OSTRZEŻENIE: Sterowanie systemem za pośrednictwem komputera nie uniemożliwia uzbrajania z aktywowanym urządzeniem. Należy zachować ostrożność podczas sterowania systemem w taki sposób!

OSTRZEŻENIE: Oprogramowanie N-Link jest dostępne wyłącznie w wersji dla systemu operacyjnego Windows.

2.10 STEROWANIE WYJŚCIAMI PG

Sterowanie wyjściami PG jest przeznaczone do funkcji niealarmowych związanych z automatyką domową. Należy się zastanowić, czy będą używane do sygnalizacji stanu czy sterowania zamkami elektronicznymi.

2.10.1 PRZYCISKI FUNKCJI NA KŁAWIATURZE

Wyjście PG włącza się przez naciśnięcie przycisku funkcji (A, B, C, D), a wyłącza przez jego ponowne naciśnięcie. Jeżeli wyjście skonfigurowano jako wyjście impulsów, wyłączy się ono w zadanym czasie.

Konieczność ewentualnego uwierzytelnienia zależy od konfiguracji systemu.

2.10.2 UWIERZYTELNIANIE Z KŁAWIATURY UŻYTKOWNIKA

Wyjście PG można aktywować przez uwierzytelnienie użytkownika (wprowadzenie kodu lub zastosowanie breloka RIFD). Wyjście PG należy skonfigurować do aktywacji za pomocą wskazanej klawiatury.

2.10.3 ZDALNE STEROWANIE

Przez naciśnięcie przypisanego przycisku na pilocie.

2.10.4 WYBÓR NUMERU

Każdy numer telefonu zapisany w centrali alarmowej (jeden użytkownik może mieć jeden numer telefonu) może sterować wyjściem PG przez wybór numeru (tj. bez rozpoczynania rozmowy). Wybór numeru obejmuje wybór numeru telefonu karty SIM używanej w systemie alarmowym i rozłączenie się, zanim system odbierze połączenie. Domyślnie system odbierze połączenie po trzecim dźwięku (około 15 sekund).

OSTRZEŻENIE: Wyjściem PG można sterować, jedynie gdy w centrali alarmowej zainstalowano komunikator GSM lub PSTN.

2.10.5 KOMUNIKAT SMS

Wysłanie wiadomości SMS może włączyć/wyłączyć dane wyjście PG. Konieczność ewentualnego uwierzytelnienia zależy od konfiguracji systemu.

Przykład: **KOD_SKONFIGUROWANY TEKST** (znak „_” = spacja)

OSTRZEŻENIE: Wyjściem PG można sterować, jedynie gdy w centrali alarmowej zainstalowano komunikator GSM lub PSTN.

3. BLOKOWANIE W SYSTEMIE

3.1 BLOKOWANIE UŻYTKOWNIKÓW

Każdego użytkownika można tymczasowo zablokować (np. jeśli zgubiono kartę/brelok lub dojdzie do ujawnienia jego kodu dostępu). Kiedy zablokowano dostęp użytkownika, centrala alarmowa nie przyjmie kodu dostępu lub karty/breloka użytkownika. Zablokowany użytkownik nie będzie także otrzymywał na telefon komórkowy powiadomień w postaci wiadomości tekstowej ani raportów głosowych.

Użytkownika może zablokować jedynie administrator systemu lub serwisant. Jednym ze sposobów odebrania praw dostępu jest wybór opcji Ustawienia / Użytkownicy / Użytkownik / Pomiń i kliknięcie „Tak” na klawiaturze LCD. Użytkownika można zablokować lokalnie lub zdalnie za pomocą oprogramowania J-Link, klikając go w kolumnie Ustawienia / Użytkownicy / Blokowanie użytkownika.

Zablokowany (dezaktywowany) użytkownik będzie oznaczony czerwonym kółkiem do chwili usunięcia blokady.

3.2 BLOKOWANIE CZUJEK

Czujkę można tymczasowo zablokować w sposób podobny do zablokowania użytkownika. Czujkę blokuje się, kiedy jej aktywacja jest niepożądana przez pewien czas (np. czujka ruchu w pomieszczeniu, gdzie znajduje się zwierzę, lub wyłączenie dźwięku syreny). Nieaktywna staje się wyłącznie funkcja alarmu, zaś system w dalszym ciągu prowadzi diagnostykę styków sabotażu i wysyła informacje o alarmie sabotażu i zdarzeniach serwisowych.

Czujkę może zablokować jedynie administrator systemu lub serwisant. W tym celu należy wybrać opcję Ustawienia / Urządzenia / Pomiń oraz Tak na klawiaturze LCD. Można także wykorzystać oprogramowanie J-Link, klikając czujkę w kolumnie Ustawienia / Diagnostyka / Nieaktywne. Zablokowana czujka pozostaje oznaczona żółtym kółkiem do chwili jej ponownego włączenia za pomocą tej samej procedury. Urządzenie można zablokować także za pomocą aplikacji mobilnej MyJABLOTRON.

OSTRZEŻENIE: Ta funkcja zależy od profilu Systemu wybranego w centrali alarmowej. Blokowanie czujek należy zawsze skonsultować z serwisantem. Jeżeli obiekt posiada ochronę fizyczną, należy skontaktować się także z agencją ochrony.

3.3 DEZAKTYWACJA KALENDARZY

Aby tymczasowo dezaktywować automatyczne, planowane zdarzenia w systemie, można wyłączyć zegary. Dezaktywacja planowanego zdarzenia (np. rozbrajanie systemu z ochrony nocnej o określonej godzinie) zapobiegnie jego realizacji (np. podczas urlopu).

Zegar można wyłączyć lokalnie lub zdalnie za pośrednictwem programu J-Link, klikając strefę w kolumnie Ustawienia / Kalendarz / Zablokowane. Nieaktywny zegar pozostaje oznaczony czerwonym kółkiem do chwili ponownego włączenia za pomocą tej samej procedury.

4. USTAWIENIA UŻYTKOWNIKA DLA CENTRALI ALARMOWEJ

4.1 ZMIANA KODU DOSTĘPU UŻYTKOWNIKA

Kody bezpieczeństwa może zmieniać wyłącznie administrator systemu i serwisant. Administrator systemu może wprowadzić zmiany za pośrednictwem menu klawiatury na wyświetlaczu LCD oraz aplikacji mobilnej.

4.2 ZMIANA, USUWANIE LUB DODAWANIE KARTY/BRELOKA RFID

Tylko administrator systemu i serwisant mogą dodawać, zmieniać lub usuwać breloki lub karty RFID z poziomu menu klawiatury na wyświetlaczu LCD. Te zmiany wprowadza się po uwierzytelnieniu, wybierając opcję Ustawienia / Użytkownicy / Użytkownik / Karta dostępu. Aby wprowadzić nową kartę/brelok RFID, należy wejść w tryb edycji (linia karty dostępu zacznie migać), naciskając Enter. Następnie należy przyłożyć do czytnika kartę/brelok RFID (przed klawiszami) lub ręcznie wpisać numer seryjny pod kodem paskowym. Po potwierdzeniu przez ponowne naciśnięcie przycisku Enter karta/brelok RFID zostanie dodana/y. Aby usunąć kartę dostępu, wpisać „0” w polu numeru seryjnego. Po zakończeniu zmianę należy zapisać, klikając Zapisz, kiedy centrala alarmowa zapyta Zapisać ustawienia?.

4.3 ZMIANA NAZWY UŻYTKOWNIKA LUB NUMERU TELEFONU

Jedynie administrator i serwisant mogą dodawać, zmieniać lub usuwać numery telefonu bądź zmieniać nazwy użytkowników z poziomu menu klawiatury na wyświetlaczu LCD. Można tego dokonać po uwierzytelnieniu, wybierając Ustawienia / Użytkownicy / Użytkownik / Telefon. Aby wprowadzać zmiany, użytkownik musi być w trybie edycji. W tym celu należy nacisnąć klawisz Enter. Wprowadzone zmiany należy potwierdzić ponownym naciśnięciem przycisku Enter. Aby usunąć numer telefonu, wpisać „0” w pole numeru telefonu. Po zakończeniu zmianę należy zapisać, klikając Zapisz, kiedy system zapyta „Zapisać ustawienia”?

4.4 DODAWANIE/USUWANIE UŻYTKOWNIKA

Jedynie serwisant może dodawać nowych użytkowników do systemu lub ich usuwać. Nowych użytkowników można dodawać do (lub usuwać z) systemu jedynie za pośrednictwem oprogramowania F-Link.

Tworząc nowych użytkowników, należy im przypisać uprawnienia do poszczególnych stref i sterowania wyjściami programowalnymi z wymaganym uwierzytelnieniem.

4.5 KONFIGURACJA ZDARZEŃ KALENDARZOWYCH

Można skonfigurować do 10 zdarzeń kalendarzowych (rozbrajanie / uzbrajanie / częściowe uzbrajanie, sterowanie lub blokowanie wyjść PG). Pojedyncze zdarzenie może łączyć kilka czynności. Na przykład można jednocześnie Uzbroić wybrane strefy, włączyć wyjście PG i zablokować inne.

Zegary można skonfigurować za pośrednictwem oprogramowania N-Link w zakładce Kalendarz.

5. HISTORIA ZDARZEŃ

System alarmowy przechowuje wszystkie zrealizowane operacje i zdarzenia (uzbrajanie, rozbrajanie, alarmy, błędy, wiadomości wysłane do użytkowników i SMA) na karcie micro SD w centrali alarmowej systemu. Każdy wpis obejmuje datę, godzinę (początku i zakończenia) oraz źródło (przyczyna/pochodzenie) zdarzenia.

Różne sposoby przeszukiwania historii zdarzeń systemu:

5.1 ZA POMOCĄ KLAWIATURY LCD

Dostęp do historii zdarzeń za pomocą klawiatury wymaga uwierzytelniania użytkownika. Po uwierzytelnieniu na klawiaturze wybierając Pamięć zdarzeń można wyświetlić dostępne opcje (zależnie od uprawnień użytkownika). Za pomocą strzałek można wyświetlać rekordy od najnowszego do najstarszego.

5.2 KORZYSTANIE Z PROGRAMU N-LINK I KOMPUTERA

Pamięć systemu można przeszukiwać za pomocą programu N-Link. Zdarzenia można wyświetlać w małych (około 1200 zdarzeń) lub większych (około 4000 zdarzeń) partiach. Zdarzenia można filtrować, zaznaczać kolorami, by ułatwić wyszukiwanie lub zapisać w pliku. Więcej informacji znajduje się w instrukcji N-Link.

OSTRZEŻENIE: Oprogramowanie N-Link jest dostępne wyłącznie w wersji dla systemu operacyjnego Windows.

5.3 LOGOWANIE DO APLIKACJI MyJABLOTRON (SIECIOWEJ/MOBILNEJ)

Wszystkie zdarzenia w systemie można wyświetlić po zalogowaniu do interfejsu sieciowego/aplikacji mobilnej MyJABLOTRON. Konto przedstawia historię w zakresie odpowiadającym uprawnieniom użytkownika.

6. CZYM JEST INTERFEJS SIECIOWY MYJABLOTRON?

Interfejs sieciowy MyJABLOTRON jest unikalną usługą umożliwiającą dostęp online do urządzeń firmy JABLOTRON. Jest on przeznaczony dla użytkowników systemu alarmowego, pozwala monitorować system i sterować nim.

INTERFEJS SIECIOWY MyJABLOTRON POZWALA UŻYTKOWNIKOM:

- Wyświetlać aktualny status systemu.
- Uzbrajać/rozbrajać cały system lub jego część.
- Sterować wyjściami programowalnymi.
- Przeglądać historię zdarzeń.
- Wysłać raporty do wybranych użytkowników za pośrednictwem SMS, poczty elektronicznej i powiadomień PUSH.
- Robić zdjęcia za pomocą czujek do weryfikacji i przeglądać je w zakładce Galeria zdjęć lub bezpośrednio w Ostatnie zdarzenia.
- Monitorować aktualną temperaturę lub zużycie energii, wraz z historią w postaci wykresu.
- Zapewnia także inne przydatne funkcje.

**7. KONSERWACJA OKRESOWA**

Należy prowadzić regularne i terminowe przeglądy konserwacyjne, pozwalające zapewnić niezawodne działanie systemu. Większą część konserwacji prowadzi firma instalacyjna nie rzadziej niż raz w roku podczas okresowych przeglądów.

Konserwacja realizowana przez użytkownika polega na zapewnieniu czystości poszczególnych urządzeń.

Niektóre urządzenia mogą wymagać regularnych testów, co opisano w instrukcjach dotyczących takich urządzeń (np. czujek pożarowych).

PARAMETR	JA-10K
Typ instalacji	Instalacja stała
Znamionowe napięcie / częstotliwość / bezpiecznik centrali alarmowej	~ 230 V / 50 Hz, T200 mA bezpiecznik 250 V 5 x 20 mm ~ 115 V / 60 Hz, T400 mA bezpiecznik 250 V 5 x 20 mm
Zakres napięcia roboczego	~ 195 V ÷ 250 V ~ 110 V ÷ 120 V
Moc / natężenie prądu	Max 23 VA / 0.1 A
Klasa ochrony	II.
Bateria awaryjna	12 V; 2.6 Ah max. (kwasowo-ołowiowa)
Niskie napięcie baterii (wskazanie błędu)	≤ 11 V
Maksymalny czas ładowania baterii	48 ÷ 72 godziny
Napięcie MAGISTRALI	12,0 ÷ 13,8 V DC / ± 100 mV
Maks. ciągłe zużycie prądu z MAGISTRALI centrali alarmowej + RJ	400 mA stale (1000 mA przez 5 minut)
Zasilanie awaryjne 12-godzinne (2,6 Ah)	LAN OFF (sieć LAN wył.): 125 mA — zużycie dla modułów zewnętrznych LAN ON (sieć LAN wł.): 85 mA — zużycie dla modułów
Maks. liczba urządzeń	32
Złącze alarmowe	MAGISTRALA JABLOTRON — dedykowane złącze przewodowe Połączenie bezprzewodowe (z JA-111R) — połączenie bezprzewodowe, protokół komunikacji JABLOTRON
Klasyfikacja systemu alarmowego	Klasa ochronności 2 / klasa środowiskowa II
@ zgodnie z normami	EN50131-1, EN 50131-3, EN 50131-6, EN 50131-5-3, EN 50131-10, EN 50136-1, EN 50136-2
@ środowisko	wewnętrzne, ogólne
@ temperatura / wilgotność pracy	-10 °C do +40 °C, wilgotność względna 75% bez kondensacji
@ moc	Typ A — zasilanie podstawowe z naładowaną baterią awaryjną
@ historia zdarzeń	około 7 milionów najnowszych zdarzeń, z datą i godziną
@ reakcja systemu na utratę komunikacji	Błąd lub sabotaż — zależnie od zadanego profilu @ MAGISTRALA — do 10 sekund @ komunikacja bezprzewodowa — w ciągu 2 godzin (raport) @ komunikacja bezprzewodowa — w ciągu 20 minut od przerywania komunikacji system blokuje się
@ reakcja na wprowadzenie nieprawidłowego kodu	Po dziesięciu nieudanych próbach wprowadzenia kodu uruchomi się alarm sabotażu. Zgodnie z wybranym profilem zablokuje on wszystkie urządzenia sterowania na 10 minut.
@ Klasyfikacja ATS	Obsługiwane klasy ATS: SP2 – SP 5, DP2 – DP3 SPT: typ Z Typ eksploatacji: Przekazujący Wbudowana sieć LAN: SP2 – SP5 (z protokołem IP) JA-190Y SP2 – SP5 (z protokołem IP) JA-190X SP2 (z protokołem Contact ID) LAN + JA-190Y DP2 – DP3 (z protokołem IP) LAN + JA-190X DP2 (z protokołem IP / CID)
@ protokoły przesyłania ATS	JABLO IP, SIA IP, Contact ID, JABLO SMS
@ ochrona ATC przed zastępowaniem i ochrona danych	protokół JABLOTRON: Szyfrowanie zastrzeżone AES z kluczem min. 128-bitowym Protokół ANSI SIA DC-09.2012 z szyfrowaniem AES 128-bitowym
Komunikator LAN	Interfejs ethernetowy CAT 5 (RJ-45)
Wymiary (mm)	268 x 225 x 83 (mm)
Waga	1450 g
Podstawowe parametry modułu JA-111R	868.1 MHz, < 25 mW, GFSK < 80 kHz
Emisje radiowe	ETSI EN 300 220-2 (JA-111R moduł)
Kompatybilność elektromagnetyczna	EN 50130-4, EN 55032, ETSI EN 301 489-1, ETSI EN 301 489-3
Bezpieczeństwo elektryczne	EN 60950-1
Warunki pracy	ERC REC 70-03, ERC DEC (98) 20
Organ certyfikujący	TREZOR TEST



ABLOTRON ALARMS a.s. niniejszym oświadcza, że centrala alarmowa JA-10K spełnia podstawowe wymagania i inne istotne postanowienia dyrektywy UE nr 2014/35/UE, 2014/30/UE oraz 2011/65/UE. Oryginał Deklaracji zgodności znajduje się na stronie www.jablotron.com w sekcji **Do pobrania**.



Uwaga: Choć niniejszy wyrób nie zawiera materiałów szkodliwych, zużyty produkt najlepiej oddać do dystrybutora lub bezpośrednio do producenta.

9. SŁOWNIK TERMINÓW

Urządzenia magistrali/bezprzewodowe

Sercem systemu alarmowego jest jego centrala alarmowa. Może się komunikować z wszystkimi urządzeniami na dwa sposoby: korzystając z magistrali, tj. przewodów do transmisji danych w obrębie strzeżonego obiektu lub jego części, bądź bezprzewodowo za pomocą komunikacji radiowej. Urządzenia magistrali są zasilane przez centralę alarmową. Urządzenia bezprzewodowe wymagają baterii, których trwałość zależy od intensywności użytkowania. Niektóre urządzenia bezprzewodowe wymagają napięcia zasilania sieciowego o wartości 230 V (patrz instrukcja danego urządzenia).

Karta / Brelok RFID

Karta / Brelok RFID umożliwia użytkownikowi obsługę systemu i służy do zbliżeniowego uwierzytelniania przez położenie karty/breloka na czytniku klawiatury. Zastępuje lub uzupełnia wprowadzanie kodu numerycznego. Kartę RFID można nosić w portfelu, który można umieścić na klawiaturze w celu uwierzytelnienia. Brelok RFID można przymocować do kluczy.

Strefa

System alarmowy można podzielić na kilka mniejszych, niezależnych części, zwanych strefami. Każda strefa może posiadać przypisane czujki, klawiatury, a także syreny, użytkowników i ich numery telefonu. W systemie może występować do 4 stref.

Wyjścia programowalne PG

System alarmowy może służyć do włączenia/wyłączenia urządzeń elektrycznych bądź sterowania nimi. W tym celu używa się wyjść programowalnych, którymi użytkownik może sterować (za pomocą wiadomości SMS, klawiatury) lub które mogą być załączane i wyłączane automatycznie, zależnie od statusu systemu (zgodnie ze statusem systemu, alarmów, błędami itp.).

Automatyka domowa

JA-100 nie tylko pełni funkcję systemu alarmowego, ale także szereg innych funkcji. Do najpopularniejszych funkcji należą: elektryczne blokady drzwi, zautomatyzowane włączniki światła z czujkami ruchu oraz zdalne sterowanie urządzeniami (ogrzewaniem, bramą garażu, bramami, szlabanami itp.).

Alarm napadowy

Alarm napadowy można uruchomić, kiedy użytkownik znajdzie się w niebezpieczeństwie i potrzebuje pilnej pomocy. Alarm napadowy można skonfigurować jako wyznaczony przycisk funkcji na klawiaturze, specjalny kod lub przycisk napadowy, bądź konkretne połączenie przycisków na pilocie. W przypadku połączenia z centrum ochrony aktywacja alarmu napadowego powoduje natychmiastową reakcję (wysłanie grupy interwencyjnej), której nie można anulować telefonicznie.

Centrum ochrony, SMA

Centrum odbioru alarmów, agencja ochrony czynna całą dobę (24/7/365) jest w stanie odpowiednio zareagować na informacje otrzymane ze strzeżonego obiektu i podjąć stosowne działania lub postąpić zgodnie z zasadami wewnętrznymi.

www.jablotron.com



MINX500300