# Контролер доступу GSM2WIEGAND v1.1

# Інструкція з інсталяції та експлуатації

Львів 2022

Зміст	
Огляд можливостей.	3
Технічні характеристики.	4
Перелік входів/виходів.	5
Встановлення.	6
Вимоги до SIM картки оператора GSM.	6
Встановлення SIM картки.	6
Підключення пристрою до джерела живлення та обладнан	ІНЯ
доступу.	7
Підключення пристрою до RFID зчитувача.	8
Підключення пристрою до зовнішньої системи контролю	
доступу.	8
Налаштування.	9
Режими роботи та світлодіодна індикація.	9
Світлодіодна індикація.	10
Ініціалізація.	11
Режим конфігурації.	11
Робочий режим	12
Мобільний застосунок і конфігурація.	13
База даних користувачів.	13
Налаштування пристрою.	14
Налаштування пристрою без мобільного застосунку.	16
Керування базою даних користувачів.	17
Сервер контролю доступу GGate.	19
Гарантія.	19
Комплект поставки.	19

# Огляд можливостей

- > Індикація рівня сигналу оператора стільникового зв'язку.
- Можливість роботи в парі з іншими системами контролю доступу (U-Prox IP400 та аналоги).
- ➢ Підтримка зовнішніх RFID зчитувачів.
- Аналоговий вхід для підключення пристрою примусового відкриття (кнопки).
- > Автоматична синхронізація часу з мережі.
- ▶ Вбудована база даних на 1000 користувачів.
- ➤ Можливість роботи з сервером контролю доступу GGate.
- Можливість автономної роботи із взаємодією з користувачем лише через мобільний додаток/СМС.
- Вбудований буфер на 500 подій, доступний для перегляду з сервера контролю доступу GGate.
- > Програмована тривалість імпульсу відкриття.
- Автоматичне вимірювання напруги живлення та перевірка балансу рахунку.
- Можливість оновлення програмного забезпечення через мережу (OTA Update).
- ▶ Індикація помилок при програмуванні.



Малюнок 1. Зовнішній вигляд пристрою

# Технічні характеристики

# Пристрій

Назва	Параметр	Одиниця виміру	Значення
Напруга живлення пристрою	Upwrdc	V	+10+15
Максимальний струм споживання	Ipwrmax	mA	1000
Струм споживання в «черговому» режимі, близько	Ipwravg	mA	50
Максимальне значення напруги лог. «1» на входах D0I, D1I	U1 <sub>maxd</sub>	V	5.75
Максимальне значення напруги лог. «1» на інших входах	U1 <sub>max</sub>	V	Upwrdc+1
Мінімальне значення напруги лог. «1» на входах D0I, D1I	U1 <sub>mind</sub>	V	3.75
Мінімальне значення напруги лог. «1» на інших входах	U1 <sub>min</sub>	V	Upwrdc*0.75
Максимальне значення напруги лог. «0» на входах D0I, D1I	U0 <sub>maxd</sub>	V	1.25
Максимальне значення напруги лог. «0» на інших входах	U0 <sub>max</sub>	V	Upwrdc*0.25
Мінімальне значення напруги лог. «0» на входах	U0 <sub>min</sub>	V	0
Максимальне значення напруги на контактах C, NO, NC	Urelmax	V	120 AC, 24 DC
Максимальний струм навантаження по виходах NO, NC	I <sub>relmax</sub>	mA	1000
Максимальний струм навантаження по інших виходах (не захищені)	I <sub>okmax</sub>	mA	200
Максимально допустима напруга на виходах D0O та D1O	Uokmaxd	V	5.75
Максимально допустима напруга на інших виходах	Uokmax	V	15
Максимальна робоча температура	t <sub>max</sub>	°C	+65
Мінімальна робоча температура	t <sub>min</sub>	°C	-20

#### GSM модем

Частотний діапазон	GSM 850/EGSM 900/ DCS 1800/ PCS1900, автоматичний вибір
Клас GSM	Small MS
Потужність	Class 4 (2W) at EGSM900/GSM850
передавача	Class 1 (1W) at DCS1800/PCS1900
SIM інтерфейс	Support SIM card: 1,8V, 3V

# Перелік входів/виходів



Малюнок 2. Перелік входів та виходів пристрою

N₂	Назва	Onuc	Призначення
1	+U_IN	«+» живлення, DC +12 V	Контакти підключення джерела
2	GND	Земля живлення	живлення
3	I1	Аналоговий вхід 1	Аналогові входи, перший - для
4	I2	Аналоговий вхід 2	примусового відкриття, другий не
5	GND	Земля аналогових входів	використовується
6	+U	Вихід живлення додаткового	
		обладнання	Виходи керування додатковим
7	OK	Вихід «відкритий колектор», дублює	обладнанням доступу
		сигнал реле	
8	С	Спільний контакт реле	Контакти реле для підключення
9	NO	Нормально відкритий контакт реле	обладнання доступу
10	NC	Нормально закритий контакт реле	
11	PROG	Перемичка режиму конфігурації	Перемичка для конфігурації пристрою

#### Таблиця 1. Перелік входів/виходів пристрою.

12	+U	Вихід живлення RFID зчитувача	
13	DOI	Вхід даних протоколу Wiegand	
		(сигнал низького рівня)	
14	D1I	Вхід даних протоколу Wiegand	
		(сигнал високого рівня)	
15	GND	Земля RFID зчитувача	Контакти підключення RFID
16	LR	Вихід керування червоним	зчитувача
		світлодіодом	_
17	LG	Вихід керування зеленим	
		світлодіодом	
18	BUZ	Вихід керування звуковим	
		індикатором	
19	HLD	Вихід блокування зчитувача	
20	GND	Земля контролера доступу	_
21	LRI	Вхід керування червоним	
		світлодіодом	
22	LGI	Вхід керування зеленим	
		світлодіодом	
23	BZI	Вхід керування звуковим	Контакти підключення зовнішнього
		індикатором	контролера доступу
24	HLI	Вхід блокування зчитувача	_
25	DOO	Вихід даних протоколу Wiegand	
		(сигнал низького рівня)	
26	D10	Вихід даних протоколу Wiegand	
		(сигнал високого рівня)	

### Встановлення

#### Вимоги до SIM картки оператора GSM.

Пристрій підтримує SIM картки стандарту GSM Phase1, GSM Phase2+ з напругою живлення 1,8 та 3,3 вольти. Це означає, що підійде довільна SIM картка оператора, виготовлена не раніше 2004 року.

SIM картка повинна бути активована, а також відмінено запит PIN коду при включенні.

#### Встановлення SIМ картки.

Під'єднайте антену до золотистого SMA роз'єму пристрою.

# УВАГА!

Вмикання пристрою без GSM антени спричиняє вихід з ладу GSM модему. Зверніть увагу – на GSM модем гарантія виробника не розповсюджується. Встановіть SIM картку в пристрій як показано на малюнку 2.



Малюнок 2. Встановлення SIM картки

# Підключення пристрою до джерела живлення та обладнання доступу.

Під'єднайте джерело живлення та принаймні один із виконавчих пристроїв доступу, як показано на малюнку 3. Виконавчий пристрій може керуватись або сигналом із виходу «ОК» (активний рівень – транзистор відкритий), або сигналами NO, NC від реле. Сигнали ОК та реле дублюються і можуть використовуватись одночасно. Вибір виходів керування залежить від типу виконавчого пристрою. Вхід I1 може використовуватись для підключення довільного зовнішнього пристрою примусового відкриття виконавчих пристроїв доступу, наприклад кнопки (низький рівень сигналу – активний).



Малюнок 3. Типова схема підключення джерела живлення та обладнання доступу

#### Підключення пристрою до RFID зчитувача.

В пристрої передбачена можливість роботи з RFID-мітками. Для цього використовується зовнішній зчитувач RFID-міток, приклад підключення типового зчитувача (напр. U-Prox SL mini) зображений на малюнку 4.



Малюнок 4. Типова схема підключення RFID зчитувача

## УВАГА!

Якщо пристрій використовується із RFID зчитувачем, переконайтесь, що типи протоколу Wiegand у налаштуваннях пристрою (див. Мобільний застосунок і конфігурація) та зчитувача співпадають.

# Підключення пристрою до зовнішньої системи контролю доступу.

Пристрій також може працювати як посередник між RFID зчитувачем та GSM модемом і зовнішнім контролером доступу. В такому разі під'єднання обладнання доступу до пристрою не обов'язкове, за умови що вся база даних і це ж обладнання доступу буде використовуватись на стороні зовнішнього контролера доступу. Типова схема підключення зовнішньої системи контролю доступу (напр. U-Prox IP400) зображена на малюнку 5.



Малюнок 5. Типова схема підключення зовнішньої системи контролю доступу

# УВАГА!

Якщо пристрій використовується із зовнішньою системою контролю доступу, переконайтесь, що типи протоколу Wiegand у налаштуваннях пристрою та системи контролю доступу співпадають. Також активуйте «прозорий режим» в конфігурації пристрою (див. Мобільний застосунок і конфігурація).

# Налаштування

Після встановлення пристрою і під'єднання усього зовнішнього обладнання можна замкнути перемичку PROG і подавати живлення. При подачі живлення пристрій ініціалізується і, за відсутності помилок (детальніше в підрозділі Ініціалізація), переходить в режим конфігурації, після цього перемичку PROG можна знімати. Під час режиму конфігурації пристрій виключно чекає СМС повідомлення з налаштуваннями (в цьому випадку номер телефону відправника не важливий) і не приймає дзвінки чи RFID мітки. Отримавши налаштування, пристрій зберігає їх та перезавантажується, переходячи в робочий режим після ініціалізації.

Щоби знову перейти в режим конфігурації на вже налаштованому пристрої, перезавантажте його та замкніть перемичку PROG на час ініціалізації пристрою. Або ж адміністратор (СМС повідомлення з номера телефону, вказаного як «адміністратор») може змінити налаштування працюючого пристрою без потреби перезавантаження вручну. Див. розділ **Мобільний застосунок і конфігурація** для детального опису всіх налаштувань і вказівок як додати і конфігурувати пристрій з допомогою мобільного застосунку чи вручну через СМС.

# Режими роботи та світлодіодна індикація



Малюнок 6. Світлодіоди індикації пристрою

### Світлодіодна індикація.

Усі світлодіоди пристрою зображені на малюнку 6, а саме зелені світлодіоди 1, 2 і 6, жовтий світлодіод 3 і червоні світлодіоди 4, 5. Світлодіоди 1 і 2 індикують рівень сигналу, світлодіод 3 показує поточні процеси роботи з мережею або конкретний тип помилки, а світлодіод 4 індикує наявність помилок та проблем із мережею. Світлодіоди 5 і 6 дублюють стан виходів LR та LG (відповідно червоний та зелений світлодіоди RFID зчитувача), а також почергово блимають коли пристрій знаходиться в режимі конфігурації.

Якщо під час ініціалізації виникає одна з передбачених критичних помилок, червоний світлодіод 4 починає горіти постійно, а жовтий світлодіод 3 показує тип помилки (див. Таблицю 2).

	Таблиця 2. Види помилок пристрою
Кількість імпульсів	Опис помилки
світлодіода З	
2	Помилка SIM картки. Очистіть контакти SIM картки або замініть її.
3	Помилка PIN коду. Відключить запит PIN коду в настройках безпеки.
4	Відсутній зв'язок з GSM модемом. Зверніться до сервісної служби
	виробника.

#### УВАГА! Пристрій знаходиться у режимі індикації помилок тільки 30 секунд. Після цього відбудеться перезавантаження GSM модему та чергова спроба ініціалізуватись.

Якщо червоний світлодіод 4 не горить постійно, то група світлодіодів 1-4 індикує стан роботи з мобільною мережею в будь-якому режимі роботи пристрою. Тоді червоний світлодіод 4 може блимати в тому випадку, якщо відсутнє покриття (чи реєстрація) стільникової мережі, або воно недостатньо для нормальної роботи пристрою. Жовтий світлодіод 3 використовується для індикації роботи GSM модему. Якщо світлодіод 3 блимає 1 раз на секунду – це свідчить, що проходить реєстрація модему в мережі оператора GSM. Світлодіод 3 блимає 1 раз на 3 секунди – модем зареєструвався в мережі. Світлодіод 3 світить із затуханням на 0,3 секунди – інтернет з'єднання з сервером контролю доступу встановлено. Якщо світлодіод 3 блимає дуже часто – іде спроба передачі даних через інтернет. Зелені світлодіод 2, 1 та червоний світлодіод 4 використовуються для індикації рівня сигналу стільникової мережі оператора. Приблизні значення рівня сигналу наведені в **таблиці 3**.

Світлодіод		Рівень	Примітки	
2	1	4		
світить	світить	не світить		Максимальний рівень сигналу.
не світить	світить	не світить		Рівень сигналу коло 50%. Достатньо для нормальної роботи пристрою.
не світить	блимає	не світить		Рівень сигналу недостатній для нормальної роботи пристрою. Необхідна зовнішня антенна.
не світить	не світить	блимає		Пристрій недієздатний. Необхідна зовнішня антенна.

Таблиця 3. Приблизні значення рівня сигналу оператора стільникової мережі.

### Ініціалізація.

Пристрій переходить в цей режим після подачі живлення. Під час ініціалізації пристрій завантажується, конфігурує GSM модем, намагається зареєструватись в мобільній мережі та читає власні налаштування з пам'яті. Ініціалізація займає близько 30 сек, в залежності від сили сигналу та часу відповіді мережі. В разі першого включення (немає налаштувань в пам'яті) або замкненої перемички PROG прилад переходить в режим конфігурації, інакше – в робочий режим. Також в ініціалізацію пристрій може перейти з інших режимів в разі повторних збоїв GSM модема з метою його перезавантажити.

Під час ініціалізації червоний світлодіод 4 блимає допоки GSM модем не зареєструється в мобільній мережі. Якщо ж світлодіод 4 починає світити постійно, це свідчить про помилку (див. підрозділ Світлодіодна індикація). Також на початку ініціалізації на декілька секунд активується вихід BUZ (звуковий індикатор RFID зчитувача, якщо підключений) для сповіщення користувача.

#### Режим конфігурації.

Перехід в режим конфігурації можливий при замиканні перемички PROG на час ініціалізації пристрою або при відсутності налаштувань пристрою (перше включення). Режим конфігурації індикують червоний і зелений світлодіоди 5 та 6, які поперемінно блимають раз на секунду.

В режимі конфігурації пристрій буде перебувати доти, доки не отримає СМС повідомлення правильного формату з налаштуваннями, або доки не буде перезавантажений. На відміну від робочого режиму, номер телефону, з якого надсилається СМС повідомлення, не перевіряється, таким чином пристрій може запрограмувати не лише адміністратор. Також в цьому режимі всі вхідні дзвінки відхиляються, а RFID мітки (якщо підключено зчитувач) ігноруються. Після успішного прийому і запису налаштувань пристрій перезавантажується самостійно.

### Робочий режим.

В робочому режимі пристрій чекає на вхідні дзвінки, СМС повідомлення та RFID мітки (якщо підключено RFID зчитувач), намагається підтримувати інтернетз'єднання з сервером контролю доступу та обмінюється з ним даними щохвилини (якщо запрограмовано, див. Мобільний застосунок і конфігурація та інструкцію до сервера).

Підтримуються три способи відчинити виконавче обладнання доступу:

1. Мобільний дзвінок на телефонний номер SIM-картки пристрою.

В такому разі пристрій перевіряє чи номер телефону користувача присутній в базі даних, не є забороненим і чи залишилась в нього хоча б одна спроба відкриття. Якщо умови справджуються, пристрій відхиляє дзвінок, відчиняє обладнання доступу і зменшує на 1 кількість спроб відкриття для цього користувача. Інакше обладнання доступу залишається зачиненим і якщо активне налаштування «грати аудіозапис», пристрій відповідає на дзвінок і відтворює відповідний аудіозапис, залежно чи номер користувача невідомий, чи присутній в базі даних, але заблокований/без спроб відкриття. Без налаштування «грати аудіозапис» всі дзвінки відхиляються і користувачу не сповіщається причина відмови в доступі.

2. RFID мітка через RFID зчитувач (якщо підключено).

Номер RFID мітки обробляється подібно до номера вхідного дзвінка, тільки зворотний зв'язок з користувачем відбувається не через мобільні дзвінки, а через світлодіоди RFID зчитувача і 5, 6 пристрою. Пристрій засвітить зелений світлодіод LG / 6 на час імпульсу відкриття (програмується в налаштуваннях) якщо доступ дозволено і червоний LR / 5 якщо в доступі відмовлено. Така індикація працює також для мобільних дзвінків і примусового відкриття.

3. Низький рівень сигналу на вході I1 (підключена кнопка / інше обладнання).

В цьому разі пристрій нічого не перевіряє, і реагує подібно до дозволеного номера телефону/RFID мітки, т. зв. «примусове відкриття». Корисно для, наприклад, відкриття дверей із середини приміщення.

Зауважте, якщо в налаштуваннях активний «прозорий режим», всі вхідні дзвінки і RFID мітки, незалежно від присутності в базі даних пристрою, додатково надсилаються до зовнішньої системи контролю доступу у вибраному протоколі Wiegand. В «прозорому режимі» керування всіма контактами RFID зчитувача також покладається на зовнішню систему контролю доступу. Решта функцій в цьому режимі працюють так само, таким чином частина бази даних (наприклад номери телефонів) може оброблятись безпосередньо пристроєм, а інша частина бази даних (наприклад RFID мітки, або навпаки) може оброблятись на стороні зовнішньої системи контролю доступу і сприйматись як невідомі номери на стороні пристрою. Обладнання доступу теж може бути різне для двох сторін.

Управління базою даних користувачів здійснюється або через СМС повідомлення від адміністратора (див. **Мобільний застосунок і конфігурація**) або через сервер контролю доступу (див. інструкцію до сервера). Також адміністратор

може змінити налаштування пристрою без необхідності переходу в режим конфігурації.

В режимі роботи з RFID зчитувачем передбачений окремий варіант додавання в базу даних RFID міток для особливих випадків, коли номер мітки невідомий і його важко визначити. Для цього на час читання мітки RFID зчитувачем потрібно замкнути перемичку PROG. Тоді пристрій автоматично запише нового користувача з цією міткою в перший вільний запис у базі даних (якщо такий є і цієї мітки немає в базі даних). Тут кількість спроб відкриття встановлюється по замовчуванню (999), її можна змінити з допомогою сервера контролю доступу. Альтернативно, щоб не відкривати корпус обладнання доступу, зімітувати замкнену перемичку PROG для наступної RFID мітки можна з допомогою CMC-команди від адміністратора (див. **Мобільний застосунок і конфігурація**).

Додатково пристрій відстежує системний час, так що при зміні дати пристрій намагається синхронізувати час з мережею інтернет (NTP сервер) для заданого часового поясу, а також перевірити баланс рахунку SIM карти (якщо задано в налаштуваннях) та синхронізувати всю базу даних з сервером контролю доступу (в режимі роботи з сервером). Зверніть увагу, що повне знеструмлення пристрою скидає системний час, тому після перезапуску пристрій намагатиметься виконати все вищезгадане протягом перших хвилин.

Якщо активне налаштування «Імпульс життя», щодня о 12:00 системного часу пристрій надсилатиме на номер телефону адміністратора СМС повідомлення з балансом рахунку SIM карти, поточною напругою живлення та системною датою і часом.

# Мобільний застосунок і конфігурація

#### База даних користувачів.

База даних пристрою містить 1000 користувачів, один запис користувача містить:

- Індекс – порядковий номер користувача в базі даних;

- Номер телефону або RFID мітки – 10 цифр (для RFID допускаються шістнадцяткові цифри) ідентифікатора, по якому користувач може отримати доступ;

- Щоденні спроби відкриття – скільки разів на день користувач може запитати доступ, максимум 999;

- Залишок спроб відкриття – скільки спроб залишилось користувачу на поточний день. Не більше щоденних спроб відкриття, встановлюється назад до щоденних при зміні дати;

- Дозвіл – по замовчуванню встановлене в «1» двійкове значення, встановлення в «0» заборонить доступ користувачу.

Основним інструментом управління базою даних є сервер контролю доступу. Також може використовуватись мобільний застосунок або СМС повідомлення вручну (не рекомендується), але лише сервер дає повний доступ до всього функціоналу пристрою і детальний контроль за всією базою даних. Так, наприклад, редагування залишку спроб відкриття і поля дозволу, чи встановлення складного графіку дозволів недоступне в мобільному застосунку.

#### Налаштування пристрою.

Для програмування налаштувань може використовуватись як мобільний застосунок GSM Wiegand (рекомендується), так і надіслане вручну СМС повідомлення.

Використовуючи застосунок, натисніть на «Список пристроїв» для управління всіма збереженими пристроями, далі натисніть на «+» для додавання нового пристрою. Ви побачите вікно з усіма налаштуваннями пристрою, як зліва на малюнку 7.

GSM Wiegand		GSM Wiegar	Видалити усіх користувачів				
Назва пристрою	GSM to Wiegand	1 Пусто	Оновити firmware				
Номер телефону пристрою	+00000000000	2 Пусто	Спроби відкриття:				
Номер телефону адміністратора	+0000000000	3 Пусто	Спроби відкриття:				
Режим роботи IP адреса/доменне ім'я сервера	Серверний • 000.000.000.000	4 Пусто	Спроби відкриття:				
Порт	00000	5 Пусто	Спроби відкриття:				
Ім'я точки доступу	internet	б Пусто	Спроби відкриття:				
Тривалість відкриття	02	7 Пусто	Спроби відкриття:				
Номер USSD	*111#	8 Пусто	Спроби відкриття:				
Відтворювати аудіозапис	Перевіряти баланс	9 Пусто	Спроби відкриття:				
Прозории режим Часовий пояс	GMT 0:00 -	10 Пусто	Спроби відкриття:				
Тип Wiegand	Wiegand 26 🔹	11 Пусто	Спроби відкриття:				
ЗБЕРЕГТИ НАЛАШТУВАННЯ	НАДІСЛАТИ НАЛАШТУВАННЯ	12 Пусто	Спроби відк +				
КЕРУВАННЯ КО	ОРИСТУВАЧАМИ	10 Пусто					
Малюнок 7. Налаштування та список користувачів пристрою							

www.glab.com.ua

Перелік усіх налаштувань:

- Назва пристрою / Device name – ім'я для поточної конфігурації пристрою, виключно для відображення в застосунку;

- Номер телефону пристрою / Device phone number – повний номер телефону SIM картки пристрою;

- Номер телефону адміністратора / Administrator phone number – повний номер телефону, позначений як «адміністратор» (зазвичай Ваш номер телефону). Тільки цей номер телефону може в подальшому бути використаний для управління базою даних користувачів і зміни налаштувань пристрою в робочому режимі;

- Режим роботи / Work mode – вибір опції Серверний / Server передбачає роботу з сервером контролю доступу GGate, вибір опції Автономний / Autonomous деактивує роботу з сервером контролю доступу. Вибирайте, якщо не збираєтесь використовувати сервер GGate, інакше наступні 2 поля обов'язкові до заповнення;

- IP адреса/доменне ім'я сервера / Server IP/Domain name – мережева адреса сервера контролю доступу або його доменне ім'я, 40 символів максимум. Порожнє поле, або нульова IP адреса еквівалентна вибраній автономній попередній опції та деактивує роботу з сервером;

- Порт / Port – номер мережевого порта, який перенаправляється до сервера контролю доступу;

- Ім'я точки доступу / АР name – ім'я інтернет точки доступу мобільного оператора, 20 символів максимум. Залежить від конкретного оператора мережі, «internet» для українських мобільних операторів;

- Тривалість відкриття / Open duration – тривалість у секундах активного імпульсного сигналу відкриття до обладнання доступу, 2 цифри максимум;

- Номер USSD / USSD number – номер USSD запиту для перевірки балансу на мобільному рахунку пристрою. Для українських операторів «\*111#»;

- Відтворювати аудіозапис / Play audio – вибір цієї опції змусить пристрій відповідати на вхідні дзвінки в разі відмови в доступі і відтворювати короткі звукові записи, що інформуватимуть користувача про причину відмови в доступі;

- Перевіряти баланс / Check balance – чи пристрій має перевіряти залишок коштів на рахунку при зміні дати за вказаним вище USSD номером;

- Прозорий режим / Transparent mode – в цьому режимі пристрій скеровує всі номери телефонів вхідних дзвінків та номери RFID міток до зовнішньої системи контролю доступу по сконфігурованому протоколу Wiegand. Також світлодіоди 5, 6 і виходи HLD, BUZ, LG, LR повторюють входи HLI, BZI, LGI, LRI відповідно (детальніше див. Робочий режим);

- Імпульс життя / Life pulse – пристрій надсилатиме на номер телефону адміністратора СМС повідомлення з балансом рахунку SIM карти, поточною напругою живлення та системною датою і часом щодня о 12:00 системного часу;

- Часовий пояс / Time zone – місцевий часовий пояс за Гринвічем (GMT), для автоматичної синхронізації часу з мережі, від -12 до 12;

- Тип Wiegand / Wiegand type – тип протоколу Wiegand, що використовується для обміну даних із RFID зчитувачем та зовнішньою системою контролю доступу (якщо підключені). Обов'язково має співпадати на всіх пристроях для коректної роботи;

Після цього конфігурацію можна зберегти кнопкою «Зберегти налаштування / Save settings» та надіслати ці налаштування пристрою кнопкою «Надіслати налаштування / Send settings».

#### Налаштування пристрою без мобільного застосунку.

Хоч і не рекомендується, але пристрій також можна запрограмувати без використання мобільного застосунку. Натомість з усіх налаштувань потрібно сформувати СМС повідомлення наступної структури:

\$SET%ADMINISTRATOR\_PHONE\_NUMBER%SERVER\_IP/DOMAIN\_NAME %PORT%AP\_NAME%OPEN\_DURATION%PLAY\_AUDIO%CHECK\_BALANCE%U SSD\_NUMBER%TRANSPARENT\_MODE%LIFE\_PULSE%TIME\_ZONE%WIEGAN D\_TYPE

Замість імен ідуть значення полів, описаних в попередньому підрозділі, в правильному порядку, розділені символом «%». Щоби вимкнути роботу з сервером (автономний режим) достатньо встановити контролю доступу поле SERVER IP/DOMAIN NAME в «000.000.000.000», поле PORT тоді значення не має. Поля, представлені в застосунку пташками (напр. LIFE PULSE) можуть приймати лише значення «0» і «1», де 0 – неактивне, 1 – активне. Поле OPEN DURATION обов'язково має складатись із 2 цифр, навіть якщо тривалість імпульсу менше 10 сек, перший «0» потрібно вказувати. Поле ТІМЕ ZONE – ціле число від «-12» до «12». Поле WIEGAND ТҮРЕ містить ціле число, що відповідає конкретному типу протоколу Wiegand, див. таблицю 4.

Приклад СМС із налаштуваннями:

\$SET%+280344598235%example.domain.com%8002%internet%02%1%1%\*111# %0%1%4%5

I would be have a second and the second seco									
Tun	Wiegand								
Wiegand	26	32	34	37	40	42	56	60	64
Значення	0	1	2	3	4	5	6	7	8
поля									

Таблиця 4. Відповідність типів протоколу Wiegand значенням поля Wiegand type.

#### Керування базою даних користувачів.

Мобільний застосунок також може використовуватись для додавання / видалення / редагування користувачів в базі даних пристрою через СМС повідомлення замість / разом з сервером контролю доступу. Зауважте, що робити це може лише адміністратор.

Щоби перейти в меню керування базою даних, потрібно вибрати налаштування конкретного пристрою і натиснути кнопку «Керувати користувачами / Manage users». В наступному вікні відображаються всі користувачі пристрою та в окремому підпункті меню вгорі (малюнок 7 з права) є команди для видалення усіх користувачів та оновлення програмного забезпечення пристрою. Обидві команди не варто використовувати без особливої потреби.

Щоби додати нового користувача – натисніть на довільне порожнє поле (кнопка «+» натомість додасть користувача в перший вільний запис). Для редагування користувача аналогічно виберіть відповідний заповнений запис. В будь-якому випадку вікно керування користувачем показане на малюнку 8.

GSM Wiegand

Ім'я користувача

Андрій Ткаченко

Номер телефону/RFID мітки

0000000000

Кількість спроб відкриття

0-999

ЗБЕРЕГТИ КОРИСТУВАЧА

#### видалити користувача

Малюнок 8. Керування користувачами пристрою.

Перелік доступних налаштувань:

- Ім'я користувача / User name – ім'я користувача, виключно для відображення в застосунку;

- Номер телефону/RFID мітки / RFID tag/phone number – або номер мобільного телефону користувача, або номер RFID мітки (шістнадцятковий, великі літери), 10 символів;

- Спроби відкриття / Open attempts – кількість спроб відкриття обладнання доступу на день для поточного користувача, 0-999;

Щоби додати чи змінити користувача, натисніть кнопку «Зберегти користувача / Save user». Натомість «Видалити користувача / Delete user» повністю видаляє запис користувача з бази даних. Зверніть увагу, додавання вже існуючого користувача видаляє попередній запис цього ж користувача, так що в базі даних не буде повторів. Видалення неіснуючого користувача не має ефекту.

## УВАГА!

3 метою збереження коштів на рахунку і мінімізації трафіку СМС мобільний застосунок не синхронізує базу даних з пристроєм. Тобто довільні зміни бази даних, здійснені або сервером контролю доступу, або іншим оновленим адміністратором, не будуть відображатись у застосунку! Тому сервер контролю доступу GGate – єдиний головний інструмент редагування бази даних з повним доступом до всіх функцій.

Як і з налаштуваннями, керувати користувачами можна через СМС вручну (не рекомендується). Щоби додати/змінити користувача надішліть на номер пристрою СМС повідомлення формату:

\$WRI%USER\_INDEX%RFID\_TAG/PHONE\_NUMBER%OPEN\_ATTEMPTS

Поле USER\_INDEX визначає порядковий номер користувача в базі даних та має містити три знаки. Розрахунок починається з 0, таким чином користувач «000» - перший, «012» - тринадцятий і т. д.

Поле OPEN\_ATTEMPTS також обов'язково має містити три символи.

Приклад:

\$WRI%013%041B00016C%008

Повідомлення видалення користувача по аналогії з попереднім виглядає наступним чином:

\$DEL%USER\_INDEX

Приклад:

\$DEL%005

СМС-команда видалення всіх користувачів:

\$DELA

СМС-команда оновлення програмного забезпечення пристрою:

\$UPD

СМС-команда додавання наступної відсканованої мітки RFID в базу даних (еквівалентна до замикання перемички PROG на час сканування):

\$ADD

# Сервер контролю доступу GGate

Сервер контролю доступу є основним (хоч і необов'язковим) інструментом взаємодії з пристроєм GSM2WIEGAND. Програмне забезпечення GGate розповсюджується вільно та працює на комп'ютерах з операційною системою Windows. Зверніть увагу, для коректного підключення пристрою до сервера через мережу, сервер повинен мати статичну IP адресу (або доменне ім'я) та відкритий порт, доступний з мережі інтернет та заданий в конфігурації пристрою.

Сервер контролю доступу має власну інтерактивну довідку, де описані, в тому числі, особливості функціоналу пристрою, доступні лише з допомогою сервера (напр. буфер подій, команди). Довідка доступна напряму в графічному інтерфейсі сервера через додаткові підпункти меню.

#### Гарантія

УВАГА! Фірма виробник несе відповідальність тільки в рамках гарантійних зобов'язань по роботі самого пристрою, та не бере відповідальність за якість виконаного монтажу пристрою, покриття та сервіс GSM оператора, якості проходження радіосигналу та ін.

Фірма виробник не несе відповідальність за довільне лихо, отримане від використання пристрою як власником, так і третіми особами.

Вся відповідальність з використання пристрою лягає на користувача.

Фірма виробник несе відповідальність з гарантійного ремонту пристрою на протязі 12 місяців з часу продажу виробу.

Гарантія не поширюється на пристрої, які вийшли з ладу з вини користувача, а саме при порушенні правил експлуатації та монтажу, при порушенні гарантійних пломб, при наявності механічних ушкоджень, а також при виході з ладу внаслідок удару блискавки, короткого замикання в мережі і т.п.

Гарантія не поширюється на модем SIM800С, що входить до складу пристрою.

#### Комплект поставки

1.Контролер доступу GSM2WIEGAND	— 1 шт.
2.Антенна ADA0068	— 1 шт.
3.Перемичка	— 1 шт.
4.Пластикові монтажні стійки	–4 шт.