



U-PROX

Контролер обмеження доступу

U-PROX IP400

Посібник зі встановлення та експлуатації

Права та їх захист

Усі права на цей документ має компанія «Limited Liability Company Integrated Technical Vision».

Торгові марки

ITV® та U-PROX® є зареєстрованими торговими марками компанії Limited Liability Company Integrated Technical Vision.

Про цей документ

Даний посібник з експлуатації описує порядок встановлення, підключення та експлуатації контролера системи керування доступом U-PROX IP400 (надалі контролер). Перед монтажем контролера ретельно вивчіть цю інструкцію.

Характеристики та параметри контролера описані у розділі **Характеристики**. У розділі **Терміни** дається пояснення термінів, що зустрічаються в даному документі.

Зовнішній вигляд контролера, опис контактів та режимів роботи наведено в розділі **Опис та робота**. Порядок монтажу, підключення зовнішніх пристроїв та налаштування контролера описані в розділі **Алгоритм роботи в локальній мережі**

Увага! Перед монтажем та підключенням контролера слід уважно вивчити цей посібник з експлуатації. Виконання монтажу, підключення контролера допускається лише особами чи організаціями, які мають відповідні повноваження від виробника.

Навчання та технічна підтримка

Курси навчання, що охоплюють питання встановлення та використання контролера U-PROX IP400, проводяться компанією «Limited Liability Company Integrated Technical Vision». Щоб отримати додаткову інформацію, зв'яжіться з персоналом «Limited Liability Company Integrated Technical Vision» за телефонами, вказаними нижче.

Технічна підтримка для всієї продукції U-PROX забезпечується в робочий час:

+38 (091) 481 01 69

support@u-prox.systems

https://t.me/u_prox_support_bot

Зазначена підтримка орієнтована на підготовлених спеціалістів. Кінцеві користувачі продукції «Limited Liability Company Integrated Technical Vision» повинні зв'язуватися зі своїми дилерами або установниками перед тим, як звертатися до «Limited Liability Company Integrated Technical Vision».

Технічна інформація доступна на сайті: www.u-prox.systems

Сертифікація

«Limited Liability Company Integrated Technical Vision» заявляє, що U-PROX IP400 відповідає Директиві про електромагнітну сумісність 2014/30/EU та Директиві 2011/65/EU (RoHS). Оригінал Декларації відповідності доступний на сайті www.u-prox.systems у розділі Сертифікати.

Зміст

Опис контролера.....	5
Призначення приладу	5
Характеристики.....	6
Терміни	7
Опис та робота	10
Будова контролера	10
Призначення контактів контролера.....	12
Перемички	13
Кнопки	13
Світлозвукова індикація контролера	13
Світлозвукова індикація зчитувачів контролера	14
Робота контролера.....	14
"Черговий" режим	15
Режим "Тривога".....	16
Режим "Вільний прохід"	16
Режим "Блокування"	17
Властивості ідентифікаторів (карток).....	17
Варіанти використання та режими роботи виходів	18
Робота комунікатора	18
Глобальний антидубль	22
Порядок роботи з пристроєм.....	25
Порядок підключення.....	26
Рекомендації щодо монтажу	26
Підключення зовнішнього зчитувача	26
Підключення шлейфів	27
Кнопка запиту проходу	28
Датчик проходу (Дверний контакт)	29
Комбінований шлейф – кнопка запиту на вихід та датчик проходу (дверний контакт)	30
Інтеграція з охоронно-пожежною сигналізацією.....	31
Виконавчі пристрої.....	32
Електрозамок.....	32
Сирени та дзвінки.....	33
Комунікація.....	33
Дротова комп'ютерна мережа (Ethernet)	34
Порядок програмування контролера	35
Сервісне обслуговування	36
Скидання в заводські установки	36

Перехід у режим програмування	37
Заміна мікропрограми пристрою	37
Заводські налаштування	37
Технічне обслуговування та ремонт	38
Гарантійні зобов'язання	38

Опис контролера

Контролер U-PROX IP400 – пристрій, призначений для керування доступом до житлових та виробничих приміщень, обліку часу проходів та подій.

Контролер поставляється у корпусі з блоком живлення.

Контролер працює з двома зчитувачами, що підключаються за інтерфейсом Wiegand.

U-PROX IP400 обробляє інформацію, що надходить зі зчитувача (зчитувачів), та за допомогою чотирьох реле здійснює комутацію виконавчих пристроїв (наприклад, замків, сирени тощо).

Наявність восьми додаткових входів з різними варіантами програмування дозволяє цілодобово контролювати вісім охоронних зон (з контролем за струмом).

Контролер може працювати як автономно, так і у складі мережі. Для об'єднання контролерів у мережу СКУД служить інтерфейс Ethernet (провідна комп'ютерна мережа).

У контролері передбачено функцію програмування мережевих налаштувань та оновлення його мікропрограми через стандартний порт USB (micro USB B).

Живлення контролера здійснюється від джерела 12В.

Контролер U-PROX IP400 має розвинені апаратні можливості та інтелектуальні функції для керування двома дверима з одним зчитувачем та кнопкою запиту проходів (двоє односторонніх дверей) або одними дверима з двома зчитувачами (двосторонні двері). Великий обсяг енергонезалежної пам'яті дозволяє використовувати контролер для організації керування доступом із кількістю постійних співробітників до 31768 чоловік та до 1000 відвідувачів (тимчасові картки).

Ретельно продумані технічні та конструкторські рішення, комунікація по комп'ютерній мережі Ethernet, енергонезалежна пам'ять та годинник реального часу, захист комунікаційних портів та портів зчитувачів від короткого замикання, перенапруги та переполюсування – все це дозволяє використовувати контролер для побудови різних систем контролю та управління доступом.

Призначення приладу

Контролер U-PROX IP400 призначений для роботи у складі систем контролю та керування доступом (СКУД) різного масштабу від СКУД невеликого офісу до прохідної великого підприємства. У СКУД контролери об'єднуються по комп'ютерній мережі.

Контролер дозволяє організувати доступ у два різних приміщення або в одне приміщення, але з контролем як входу, так і виходу, а також систему сигналізації приміщень, пов'язаних з даними точками проходу. У разі одночасного контролю входу та виходу з приміщення забезпечується функція "Антидубль".

Характеристики

- Живлення - зовнішнє джерело 12В:
 - Струм споживання від джерела 12 В (при відключених навантаженнях), не більше 160 мА
 - Амплітуда пульсацій джерела живлення постійного струму, не більше 500 мВ
- Можливість підключення зовнішніх зчитувачів безконтактних ідентифікаторів, які працюють у протоколі Wiegand 26, 32, 34, 37, 40, 42, 56, 58, 64, 80 бітів.
- Вісім входів для підключення шлейфів з контролем струму (кінцевий резистор – 2,2 кОм)
- Два реле (контакти NO, NC, COM) 5 А @ 24 В
- Два реле (контакти NO, COM) 1 А @ 24 В
- Один порт USB для конфігурації мережевих налаштувань (для зв'язку із сервером СКУД) та оновлення його мікропрограми через стандартний порт USB (micro USB B).
- Контролює відкриття корпусу приладу
- Порт Ethernet 10BASE-T/100BASE-TX
- Повна конфігурація виконується за допомогою СКУД через комп'ютерну мережу
- Годинник реального часу
- Функція Антидубль
- Енергонезалежна пам'ять:

Ідентифікаторів	31768
подій	47000
Тайм-зон	250
Тижневих розкладів	250
свят	250
Тимчасових ідентифікаторів	1000

Терміни

Ідентифікатори

У системах керування доступом кожен користувач має ідентифікатор із унікальним кодом. Ідентифікатори можуть мати вигляд пластикової картки, брелока та ін.

Зчитувач

Для читання кодів ідентифікаторів призначено зчитувачі, що підключаються до контролера СКУД.

Існує кілька поширених типів ідентифікаторів та зчитувачів для них. При підключенні до контролера важливо, щоб відповідав тип інтерфейсу між зчитувачем та контролером. Для підключення до контролера U-PROX IP400 використовується інтерфейс Wiegand.

PIN-код

Якщо зчитувачі мають вбудовану клавіатуру, то ідентифікатором може виступати код, що вводиться з клавіатури. Зазвичай цей код називають PIN-кодом, він може бути самостійним ідентифікатором або служити доповненням до картки або брелока, тоді після пред'явлення картки зчитувач "очікує" введення PIN-коду.

Двері

Місце, точка доступу, де безпосередньо здійснюється контроль доступу (наприклад двері, турнікет, кабіна проходу, обладнані необхідними засобами контролю).

Точка доступу

Див. Двері.

Точка проходу

Точка проходу - це логічна одиниця СКУД, що управляє проходом через двері в одному напрямку і включає зчитувач, контролер (або частину контролера), виконавчий механізм. Таким чином, турнікет із контролем проходу в обидві сторони складає дві точки проходу, а двері зі зчитувачем лише з одного боку – одна точка проходу. Двері, що складаються з двох точок проходу, називаються двосторонніми, а двері, що складаються з однієї точки проходу – односторонніми.

Кнопка запиту на вихід

У разі односторонніх дверей для виходу з приміщення використовується кнопка, підключена до контролера – кнопка запиту на вихід. Відкриття дверей будь-яким іншим способом: натисканням кнопки на електрозамку, за допомогою ключа і т.д. - приводить до виникнення події ЗЛОМ ДВЕРЕЙ.

Кнопка запиту на вихід може також використовуватись для дистанційного відчинення дверей.

Датчик проходу (Дверний контакт)

Правильно спроектована СКУД має контролювати стан точки проходу: положення дверного полотна, стріли шлагбауму, ротора турнікету тощо. Завдяки цьому СКУД може запобігати ситуації, коли по одному ідентифікатору проходить кілька людей, двері після проходу користувача залишилися відчиненими і т.д.

Для цього до входу контролера підключається магнітний датчик закриття дверей, датчик положення ротора турнікета, датчик положення стріли шлагбаума. Вхід, до якого підключаються ці датчики, називається вхід датчика проходу (або дверного контакту).

Антидубль (AntiPassBack)

У контролері передбачена функція антидубль, яка необхідна для запобігання ситуації, коли один користувач, пройшовши через двері, керовані СКУД, в одному напрямку, передає свій ідентифікатор іншому користувачу. Якщо цю функцію увімкнено, то контролер відстежує положення ідентифікатора – всередині/зовні. При спробі повторного проходу в одному напрямку контролер СКУД відмовляє у доступі і генерує повідомлення У ДОСТУПІ ВІДМОВИНО, АНТИДУБЛЬ.

Увімкнути функцію антидубль можна лише якщо контролер керує двосторонніми дверима.

Глобальний антидубль (AntiPassBack)

Відстеження переміщення ідентифікатора через усі підконтрольні двері. При глобальному антидублі виконується поділ об'єкта на зони доступу, прохід яких можливий через кілька дверей. При спробах повторного проходу, несанкціонованого використання ідентифікатора в даних зонах контролери СКУД відмовляють у доступі та генерують повідомлення ГЛОБАЛЬНИЙ АНТИДУБЛЬ: У ДОСТУПІ ВІДМОВЛЕНО.

Інтервал "час проходу"

При порушенні дверного контакту, точка проходу переходить у режим "Тривога" (див. Режим "Тривога"нижче). Тривога не включається, якщо контакт порушено під час інтервалу "час проходу". Інтервал починається, коли контролер дозволяє прохід користувачеві. Тривалість інтервалу задається під час програмування. Також час проходу закінчується при порушенні та подальшому відновленні дверного контакту.

Спроба підбору ідентифікатора

У контролері передбачена функція, що включає режим тривоги, якщо кілька разів поспіль було пред'явлено ідентифікатор, що не зареєстрований в системі. Показ зареєстрованого ідентифікатора скидає лічильник кількості спроб підбору ідентифікатора. При програмуванні контролера можна увімкнути цю функцію і вказати кількість пред'явлень.

Розклади

При налаштуванні прав доступу користувачів вказуються інтервали часу та дати, за якими дозволяється прохід.

У контролері може зберігатися до 250 часових інтервалів, із цих часових інтервалів можна становити до 250 тижневих розкладів.

Крім того, існують святкові дні, що зустрічаються раз на рік, таких дат у контролері може бути задано до 250.

Таймзони (часові інтервали)

Таймзона є складовою розкладу, і служить організації часових інтервалів і зв'язування їх з правами доступу. Служать для перевірки прав доступу та для виконання інших функцій, що базуються на розкладах.

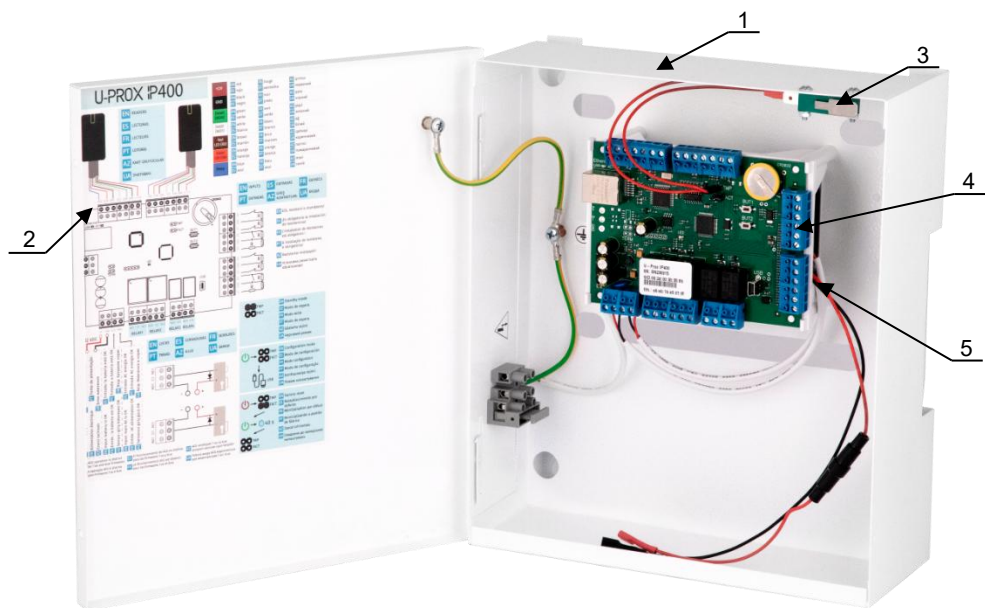
Завантаження

Після програмування входів, виходів, прав доступу для власників ідентифікаторів та інших параметрів контролера необхідно завантажити контролер. Під час завантаження дані про налаштування потрапляють з комп'ютера до контролера.

Опис та робота

Будова контролера

Зовнішній вигляд пристрою представлений Мал. 1.



1. Корпус пристрою
2. Дверця корпусу
3. Тампер (датчик розкриття)
4. Контролер
5. Блок живлення

Рис. 1. Зовнішній вигляд U-PROX IP400

Розташування на платі контролера перемичок (джамперів), кнопок і знімних колодок з роз'ємами та їх призначення показано на Мал. 2.

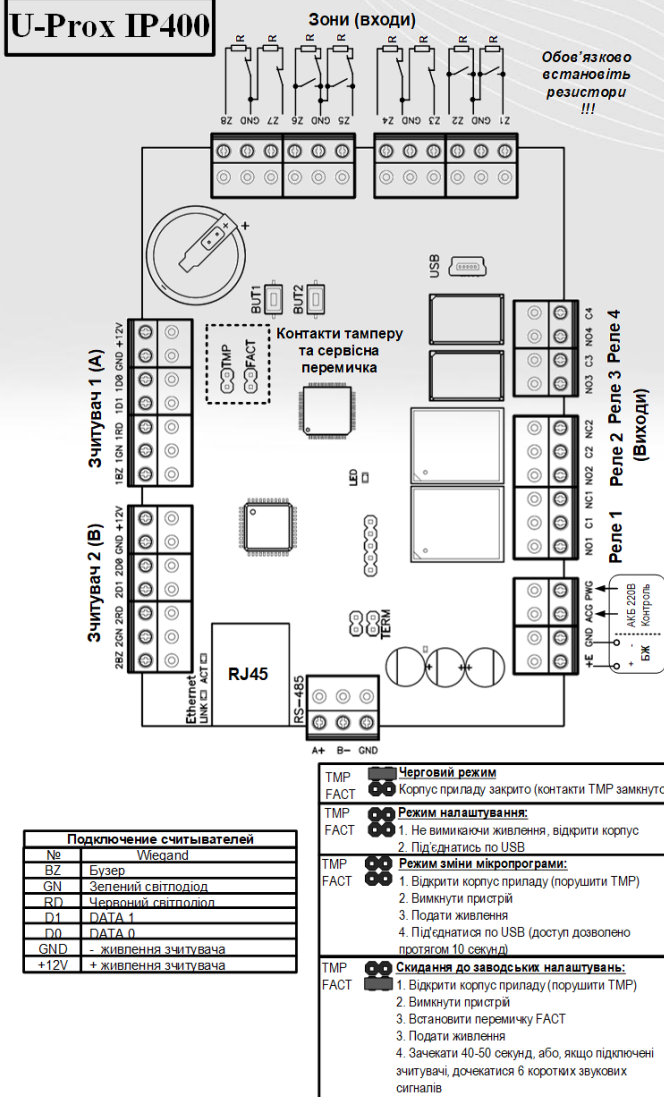


Рис. 2. Зовнішній вигляд плати контролера

Призначення контактів контролера

Контакт	Назва	Призначення
Z1	Z1	Контакти для підключення шлейфів
Z2	Z2	
Z3	Z3	
Z4	Z4	
Z5	Z5	
Z6	Z6	
Z7	Z7	
Z8	Z8	
GND	GND	
NC1	нормально замкнутий	Контакти реле 1
NO1	нормально розімкнений	
C1	Загальний	
NC2	нормально замкнутий	Контакти реле 2
NO2	нормально розімкнений	
C2	Загальний	
NO3	нормально розімкнений	Контакти реле 3
C3	Загальний	
NO4	нормально розімкнений	Контакти реле 4
C4	загальний	
1BZ	бузер	Підключення виносного зчитувача 1 (Точка проходу А)
1GN	зелений світлодіод	
1RD	червоний світлодіод	
1D1	Data 1	
1D0	Data 0	
+12 V	Живлення	
GND	GND	
2BZ	бузер	Підключення виносного зчитувача 2 (Точка проходу В)
2GN	зелений світлодіод	
2RD	червоний світлодіод	
2D1	Data 1	
2D0	Data 0	
+12 V	Живлення	
GND	GND	
E+		Підключення зовнішнього джерела живлення
GND		
ACG	Акумулятор в нормі	Сигнали від джерела живлення
PWG	Мережа 220В у нормі	

TMP	Тампер	Датчик розкриття корпусу
Роз'єм USB		
USB Micro B	USB роз'єм	Використовується для початкової конфігурації мережних налаштувань та оновлення мікропрограми

Перемички

Сервісні

- TMP – тампер (датчик розтину корпусу)
- FACT - скидання в заводські установки

Кнопки

- BUT1 – кнопка запиту проходу для точки проходу А
- BUT2 - кнопка запиту проходу для точки проходу В

Світлозвукова індикація контролера

Жовтий світлодіод - LED:

- **черговий режим (періодичне миготіння):**
 - **1 короткий імпульс раз на секунду** – зв'язок із сервером СКУД у нормі;
 - **2 короткі імпульси раз на секунду** – зв'язок із сервером СКУД відсутній
- **часте миготіння** – відбувається завантаження даних із сервера
- **режим завантаження:**
 - **світлодіод включений протягом 5 секунд** - детектування відкриття корпусу (порушення TMP), вхід у режим завантажування
 - **часте миготіння** – очікування в режимі завантажування (одягнута перемичка FACT), також така індикація встановлюється при невдалій спробі оновлення мікропрограми
 - **6 коротких звукових сигналів** - успішне завантаження мікропрограми
 - **2 короткі звукові сигнали** – вихід із режиму завантаження
- **6 коротких звукових сигналів** (при відкритому корпусі (порушеному TMP) та закороченій перемичці FACT) – зроблено скидання в заводські установки

Світлодіод **Link** :

- світиться - Ethernet кабель справний

Світлодіод **Act.:**

- часте миготіння – відбувається обмін даними

Світлозвукова індикація зчитувачів контролера

Індикація режимів доступу здійснюється за допомогою зчитувачів контролера. Для кожного контролера може бути виконано індивідуальне налаштування індикації з програмного забезпечення СКУД. Налаштування представлені у вигляді таблиці з комбінаціями звукової та світлової індикації.

Значення індикації за замовчуванням:

Режим	Індикація зчитувачів
Черговий режим	Без звуку, миготіння червоним 1 раз на секунду
Контроль PIN-коду увімкнено	Без звуку, миготіння червоний-зелений 1 раз на секунду
Вільний прохід	Без звуку, миготіння зелений-жовтий 1 раз на секунду
Блокування	Без звуку, миготіння червоний-жовтий 1 раз на секунду
Тривога	Без звуку, червоний безперервно
Реєстрація картки	Без звуку, миготіння зелений 1 раз на секунду
Ініціалізація	Без звуку, без світлової індикації
Завантаження	Без звуку, червоний безперервно
Очікування введення PIN-коду	Без звуку, миготіння жовтий 1 раз на секунду
Доступ дозволено	Без звуку, зелений безперервно
Доступ заборонено	Звук безперервно, червоний безперервно

Робота контролера

Контролери поставляються у незавантаженому стані, у заводських налаштуваннях. У цьому стані жовтий світлодіод на контролері блимає 1 раз на секунду. Для роботи контролера в СКУД необхідно завантажити в нього мережеві налаштування за допомогою програми "Конфігуратор".

Увага! Рекомендуємо встановити на всі входи контролера резистори (з комплекту).

Після завантаження налаштувань у контролер, і за умови не порушених входів, контролер переходить у режим **"Черговий"**.

Скидання контролера в незавантажений стан здійснюється лише командою з комп'ютера, див. інструкцію з програмування.

Контролер може керувати двома незалежними точками проходу. Точка проходу може бути в чотирьох режимах: **"Черговий"**, **"Тривога"**, **"Блокування"** і **"Вільний прохід"**. Найвищий пріоритет у режиму **"Вільний прохід"**, оскільки цей режим включається у разі пожежі, потім йдуть режими **"Блокування"**, **"Тривога"** та **"Черговий"**.

"Черговий" режим

Черговий режим – це основний режим роботи контролера. У цьому режимі контролер надає чи відмовляє у доступі власникам ідентифікаторів.

Прохід при пред'явленні ідентифікатора

Для проходу через двері користувач підносить безконтактний ідентифікатор до зчитувача. Якщо ідентифікатор зареєстрований і зараз прохід дозволено, то двері відчиняються (контролер активує виконавчий механізм).

Прохід при пред'явленні ідентифікатора та PIN-коду

Після пред'явлення зареєстрованого ідентифікатора контролер перевіряє, чи потрібне введення PIN-коду і, якщо потрібно, то включається очікування введення PIN-коду. Після введення правильного PIN-коду відкривається точка проходу (активується виконавчий механізм).

Прохід кнопкою запиту проходу (дистанційного відкриття дверей)

Вихід із приміщення з односторонньою точкою проходу або пропуск відвідувачів відбувається за допомогою кнопки запиту проходу. Натискання та відпускання кнопки запиту проходу відкриває точку проходу (активується виконавчий механізм).

Відмова у доступі при пред'явленні ідентифікатора

Власнику ідентифікатора може бути відмовлено у доступі з таких причин:

- контролер перебуває у незавантаженому стані
- картка не зареєстрована у контролері
- термін дії картки минув
- на даний час та/або день тижня доступ заборонено
- спроба повторного проходу при включеній функції "Антидубль"
- пред'явлено ідентифікатор, зареєстрований як загублений або заблокований
- контролер знаходиться в режимі "Тривога"
- контролер знаходиться в режимі "Блокування" ,
- термін початку дії тимчасової картки ще не настав,
- вичерпано лічильник проходів для тимчасової картки (картка відвідувача).

Режим "Тривога"

Точка проходу переходить у режим **"Тривога"** при несанкціонованому проході (злом проходу), відкритті корпусу контролера, пред'явленні ідентифікатора, записаного як загублений, якщо двері відкриті занадто довго (перевищено час відкритого стану дверей) і якщо включена відповідна функція підбору ідентифікатора.

У режимі **"Тривога"** контролер активує виходи, призначені як ТРИВОГА та СИРЕНА. Тривожний вихід залишається активованим до вимкнення режиму **"Тривога"**, а виходу, призначеному як СИРЕНА, програмується час звучання сирени.

Якщо точка проходу перебуває у режимі **"Тривога"**, то прохід крізь нього заблоковано. Двері можуть бути відчинені натисканням кнопки запиту на вихід. Вимкнути режим **"Тривога"** можна пред'явленням ідентифікатора, що має ознаку **"Зняття тривоги"** або за командою з комп'ютера.

Режим "Вільний прохід"

При експлуатації СКУД бувають ситуації, коли необхідно відкрити двері для вільного проходу людей, наприклад, у разі пожежі, землетрусу чи іншої екстремальної ситуації. Для цього випадку в контролері передбачено режим **"Вільний прохід"**.

Точка проходу переходить у режим **"Вільний прохід"** за командою оператора з комп'ютера або порушенням шлейфу, призначеного як ВІЛЬНИЙ ПРОХІД. Точка проходу залишається в режимі **"Вільний прохід"** до тих пір, поки порушений шлейф ВІЛЬНИЙ ПРОХІД (якщо шлейф порушений, скасувати стан ВІЛЬНИЙ ПРОХІД по команді оператора не можна).

Контролер дозволяє налаштувати шлейф на функцію ВІЛЬНИЙ ПРОХІД для точки проходу А, В або двох точок разом (А+В).

Протягом усього часу, поки точка проходу знаходиться в режимі **"Вільний прохід"**, замок утримується у відкритому стані, контролер реєструє пред'явлення ідентифікаторів, введення кодів та зберігає за ними в журнал подію «Доступ надано», незалежно від стану антидублю, розкладу, тощо. Це використовується для контролю наявності персоналу у приміщеннях у разі екстремальної ситуації.

Для забезпечення режиму вільного проходу при використанні замикаючих пристроїв з механічним перевзводом обов'язково потрібно контролювати стан дверей. Замикаючі пристрої з механічним перевзводом відмикаються імпульсом струму і залишаються у відчиненому стані, поки двері не будуть зачинені. В момент закриття дверей замикаючий пристрій переходить у закритий стан. Контролер у режимі **"Вільний прохід"** перевіряє стан дверного

контакту і після кожного закриття дверей знову подає відмикаючий імпульс на замок.

При роботі контролера без дверного контакту (геркона) використання типу виходу «імпульсний» для відмикання замка не рекомендовано. Режим **"Вільний прохід"** в даному випадку не працюватиме коректно - відчинити двері без піднесення ідентифікатора неможливо.

Режим "Блокування"

При виникненні ситуації, яка потребує заблокувати двері для всіх користувачів системи, в контролері вмикається режим **"Блокування"**. Якщо точка проходу знаходиться в режимі **"Блокування"**, прохід через нього дозволяється тільки власникам ідентифікаторів з ознакою **"Служба безпеки"**. Двері не можуть бути відчинені натисканням кнопки запиту на вихід.

Точка проходу переходить у режим **"Блокування"** за командою оператора з комп'ютера або порушенням шлейфу, призначеного як БЛОКУВАННЯ. Точка проходу залишається в режимі **"Блокування"** до тих пір, поки порушено шлейф БЛОКУВАННЯ (якщо шлейф порушено, скасувати стан БЛОКУВАННЯ за командою оператора не можна).

Контролер дозволяє налаштувати шлейф на функцію БЛОКУВАННЯ для точки проходу А, точки проходу В, або для двох точок разом (А+В).

Властивості ідентифікаторів (карток)

Код (електронний код картки)

Кожна картка має свій унікальний код, який задається під час виготовлення. Складається із 10 шістнадцяткових цифр.

PIN-код

Додатковий код, призначений для картки. Повинен складатися лише з шести десяткових цифр. Може використовуватися разом із зчитувачами, які мають вбудовану клавіатуру.

Після піднесення картки до зчитувача на вбудованій клавіатурі зчитувача необхідно ввести PIN-код і натиснути кнопку «#». Якщо введено правильний PIN-код, то контролер відімкне двері і надасть доступ. В іншому випадку контролер видасть попереджувальний сигнал, в журналі буде зареєстрована подія «Неправильний PIN-код», а двері залишаться замкненими.

Термін дії

Дата закінчення терміну дії картки.

Зняття тривоги

При піднесенні такої картки до зчитувача дверей, що знаходяться у тривожному стані, контролер реєструє подію «Завершення стану ТРИВОГА» і переводить

двері до чергового стану. Якщо ж до зчитувача піднести картку, яка не має права зняти тривогу, то двері залишаться в тому ж стані, а в журналі реєструється подія «Прохід заборонено. Стан тривоги».

Служба безпеки

Право проходу через заблоковані двері.

Якщо двері перебувають у стані «Блокування», то піднесення звичайної картки призводить до реєстрації події «Прохід заборонено. Стан БЛОКУВАННЯ». Під час піднесення картки з атрибутом «Служба безпеки» контролер надасть доступ та зареєструє подію «Прохід дозволено. Стан БЛОКУВАННЯ».

VIP

Право проходу завжди і скрізь, крім випадку, коли двері перебувають у стані блокування.

Картці з цією ознакою може бути призначений будь-який розклад, на неї не поширюється антидубль та обмеження терміну дії. Вона може мати пінкод.

Якщо двері перебувають у стані «Блокування», то ідентифікатору з цією ознакою контролер не надає доступу.

Антидубль вимкнено

Право проходу без урахування режиму антидублів. Доступ до такої картки буде надано незалежно від напрямку попереднього проходу, але з урахуванням призначеного розкладу та інших ознак, призначених для картки.

Варіанти використання та режими роботи виходів

Всі виходи контролера можуть бути довільно запрограмовані на кілька варіантів використання: **замок, сирена, тривога, програмований вихід**. Крім того, для кожного виходу програмується режим роботи: **старт-стопний** (вихід залишається активованим, поки присутня відповідна умова, наприклад, протягом усього часу, поки контролер перебуває в режимі "Тривога"), **імпульсний** (вихід активується на запрограмований час), **тригерний** (за першою подією вихід активується за наступним вимикається і т.д.), **безперервний** (вихід активується або деактивується окремими командами).

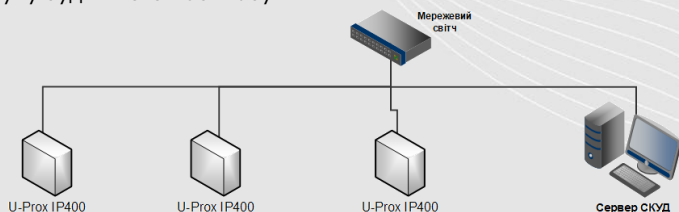
Робота комунікатора

Контролер U-PROX IP400 працює в автоматичному режимі. Після завантаження даних із сервера виконується відпрацювання правил доступу для пред'явлених карток і повідомлення про події доступу надсилаються на сервер.

Комунікатор контролера працює в режимі **нотифікації**, тобто за наявності події (прохід, порушення зони) ініціюється передача даних на сервер СКУД.

Контролер U-PROX IP400 може бути підключений до комп'ютерної мережі за допомогою дротового з'єднання (Ethernet). У цьому випадку забезпечується як робота всередині **локальної** мережі підприємства (див. рис 3), так і **через**

мережу Інтернет (див. Мал. 4), що дозволяє будувати розподілені системи доступу будь-якого масштабу.



Мал. 3. Приклад локальної мережі

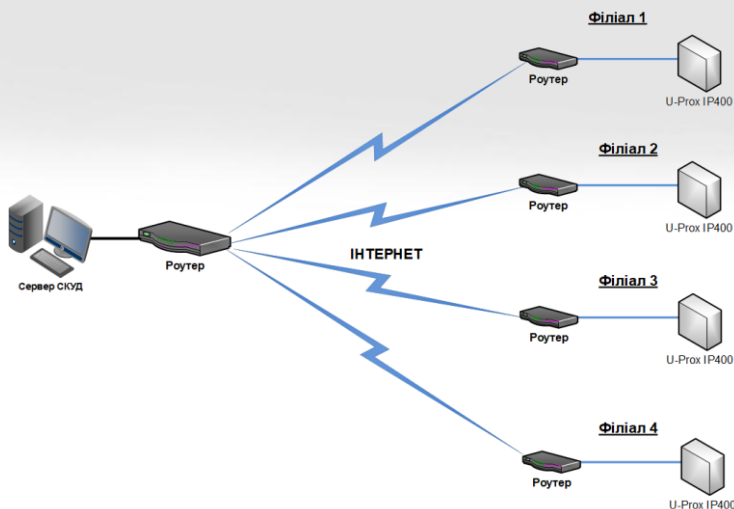


Рис. 4. Приклад розподіленої мережі

При побудові спільної мережі центрального офісу та філій для додаткового захисту рекомендується використовувати VPN технології, а для резервування каналів зв'язку - роутери з двома різнорідними каналами доступу до Інтернету.

Алгоритм роботи всередині локальної мережі

1. Після включення контролера виконується перевірка, увімкнено режим DHCP (IP адреса приладу 0.0.0.0) чи прилад отримав статичну IP адресу;
2. Якщо увімкнено режим DHCP, буде запущено процедуру динамічного призначення IP-адреси;

3. Періодичне оновлення статусу IP адреси (продовження зарезервованої IP адреси, якщо увімкнено режим DHCP);
4. Визначення доступності сервера СКУД і контролера U-PROX IC A (по IP або DNS імені);
5. Періодичне відправлення тестових сигналів;
6. Надсилання повідомлень про події доступу;
7. Очікування команд;

Алгоритм роботи через мережу Інтернет (локальна дротова мережа)

1. Після включення контролера виконується перевірка, увімкнено режим DHCP (IP адреса приладу 0.0.0.0) чи прилад отримав статичну IP адресу;
2. Якщо увімкнено режим DHCP, буде запущено процедуру динамічного призначення IP-адреси;
3. Періодичне оновлення статусу IP адреси (продовження зарезервованої IP адреси, якщо увімкнено режим DHCP);
4. Визначення можливості виходу в Інтернет (доступність IP адрес маршрутизаторів);
5. Визначення доступності сервера СКУД і контролера U-PROX IC A (по IP або DNS імені);
6. Періодичне відправлення тестових сигналів;
7. Надсилання повідомлень про події доступу;
8. Очікування команд;

Автоконфігурація контролерів в одноранговій мережі

Використання мережної існуючої інфраструктури, стандартних мережевих протоколів (наприклад, DHCP) дозволили реалізувати принцип "підключив і працюєш". Режим автоконфігурації адреси сервера на пристроях значно полегшує розгортання системи контролю доступу (див. Мал. 5).

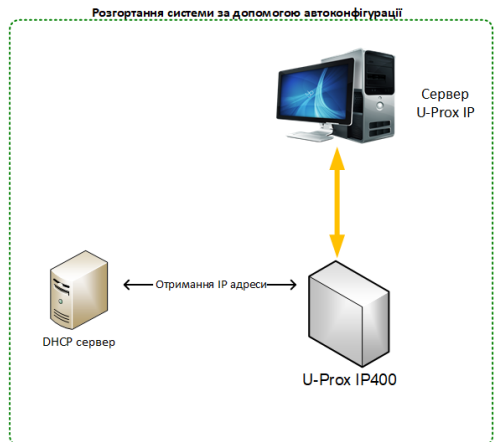


Рис.5. Автоконфігурація пристрою

Автоконфігурація адрес сервера

1. Після включення контролера, виконується перевірка, чи увімкнено режим DHCP (IP адреса приладу 0.0.0.0), чи прилад отримав статичну IP адресу;
2. Якщо увімкнено режим DHCP, буде запущено процедуру динамічного призначення IP-адреси;
3. Якщо не встановлено адресу сервера СКУД (IP або DNS ім'я), включається режим автоконфігурації контролера:
 - a. Прилад виконує розсилку пакетів даних, що сповіщають сервер СКУД про себе як новий пристрій у локальній мережі.

Хоча дана розсилка широкомовна, але вона обмежена одноранговою локальною мережею та активним мережевим обладнанням. Тому для мереж зі складною топологією IP адреси сервера СКУД задаються вручну.

- b. При отриманні пакета даних від нового приладу оператор системи буде видано оповіщення. Далі оператор повинен додати пристрій до бази даних (БД).
- c. Після додавання пристрою до БД прилад отримує пакет з відповіддю від сервера СКУД. Ініціалізується запис адреси сервера в налаштування контролера і припиняється широкомовне розсилання.
- d. Після налаштування параметрів контролера в БД оператор повинен завантажити пристрій. Прилад буде пов'язаний із цією СКУД, що виключить можливість перехоплення управління.

Щоб скасувати прив'язку контролера, його слід скинути до заводських установок.

- e. У разі зміни адреси сервера пристрій повторно виконає автоконфігурацію, але обмін даними буде можливий тільки зі СКУД, до якої був прив'язаний прилад.

Глобальний антидубль

Контролер U-PROX IP400 може працювати у складі системи глобального антидублю. У такому випадку головний контролер серії U-PROX IC A відстежує місцезнаходження особи за фактом проходження через двері, отримуючи дані від контролерів серії U-PROX IP400.

Основою роботи глобального антидублю є зонний антидубль. Приміщення об'єкту поділено на кімнати – зони доступу. За такого розподілу вхід до іншої зони є виходом з попередньої. Прохід до зони можливий через різні двері.

Контролер антидубля відстежує переміщення співробітників із зони до зони, отримуючи дані від контролерів доступу. При цьому відстежується місцезнаходження особи, яка може мати кілька ідентифікаторів (див. мал. 6).

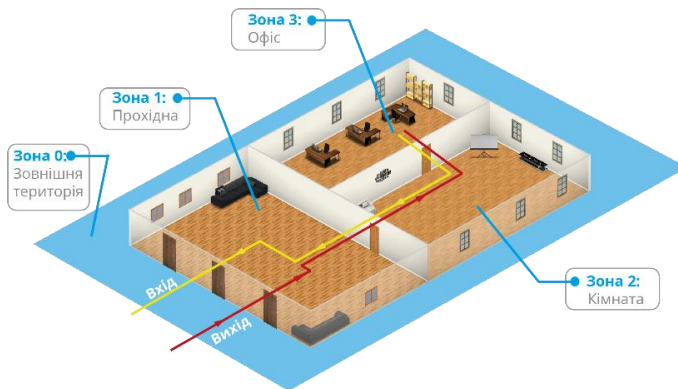


Рис. 6. Розподіл зон доступу

Спочатку співробітник (персона) має положення "Не визначено" і тільки після першого піднесення ідентифікатора до зчитувача його місцезнаходження фіксується контролером U-PROX IC A.

Розташування «Не визначено» присвоюється під час реєстрації нового співробітника або після команди оператора системи «загальне скидання розташування».

За допомогою системи глобального антидублю можливе припинення повторного проходження, використання дублікатів карток, проникнення (несподівана поява всередині), передачі ідентифікатора іншим особам тощо. (див. мал. 7):



Рис. 7. Відстеження порушень

У разі втрати зв'язку з контролером СКУД, злому дверей, переходу дверей у вільний прохід, тощо, контролер антидубля поєднує зони доступу в одну, вважаючи, що персонал може знаходитися і там, і там.

По відновленню дверей або зв'язку з контролером – зони роз'єднуються. Фактичне розташування персоналу в них визначається за подальшим піднесенням ідентифікатора до читувача (див. мал. 8).

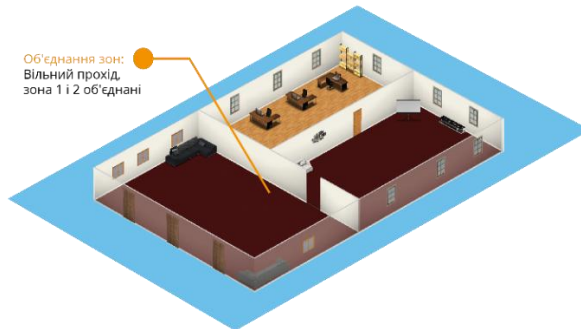


Рис. 8. Об'єднання зон доступу

При втраті зв'язку з контролером U-PROX IC A контролери доступу U-PROX IP400 можуть бути налаштовані на два варіанти поведінки:

- Нікого не пускати
- Пускати згідно даних про положення особи для локального антидублю

Вимоги до налаштування контролера U-PROX IC A

- Контролер повинен мати статичну (фіксовану) IP адресу

Вимоги до налаштування контролерів U-PROX IP400

- У глобальному антидублі беруть участь лише контролери з двосторонніми дверима (вхід та вихід за пред'явленням ідентифікатора)
- Першою адресою сервера СКУД у налаштуваннях комунікації приладу має бути вказана адреса комп'ютера із серверним ПЗ U-PROX IP
- Другою адресою сервера СКУД у налаштуваннях комунікації приладу має бути вказана адреса контролера U-PROX IC A
- У U-PROX IP для дверей повинен бути включений режим антидублю "Загальний"
- У U-PROX IP контролеру доступу повинен бути вказаний провідний контролер антидублю та реакція на втрату зв'язку з ним.

Контролери U-PROX IP400 виконують надсилання повідомлень про події доступу на дві адреси одночасно. Перша адреса – сервер СКУД, для відображення та зберігання подій у БД програми. Друга адреса - контролер U-PROX IC A, що відправляє у відповідь команду на заборону або надання доступу.

Після пред'явлення ідентифікатора затримка на надання чи відмова у доступі може становити до 1 секунди в залежності від топології та пропускну́ї спроможності комп'ютерної мережі

Порядок роботи з пристроєм

Контролер поставляється в металевому корпусі з джерелом живлення.
Габаритні розміри приладу наведено на мал. 9.

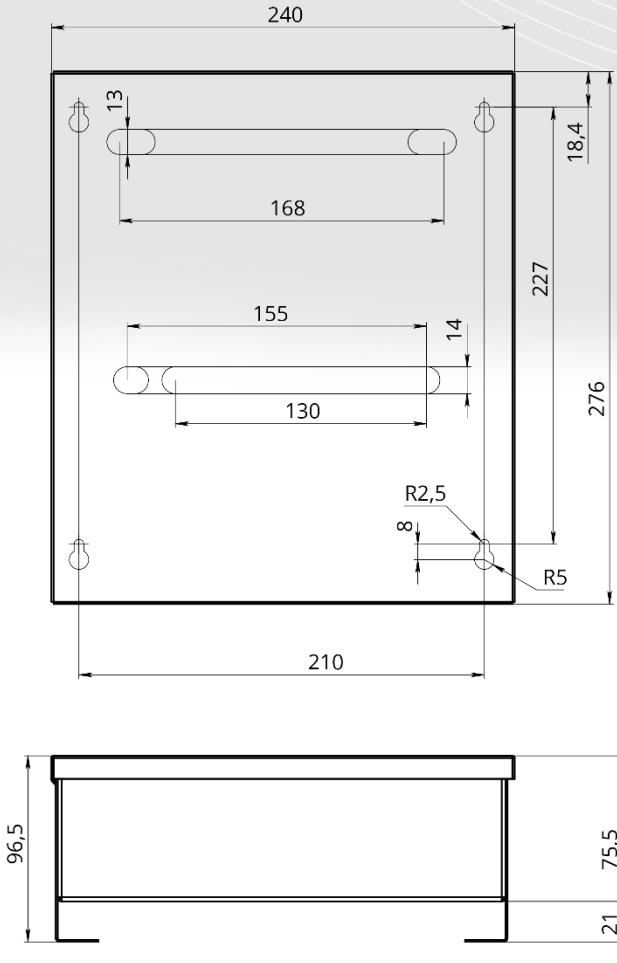


Рис. 9. Габаритні розміри та розмітка отворів кріплення

Порядок підключення

1. Перед встановленням зробіть початкове налаштування (а саме встановіть параметри мережевих налаштувань) контролера за допомогою утиліти "Конфігуратор" через USB порт
2. У місці встановлення контролера виконайте підготовку - розмітьте та просвердліть отвори (див. **Рекомендації щодо монтажу**)
3. За необхідності виконайте підведення кабелю від блока живлення
4. Виконайте підведення кабелю від виконавчих пристроїв (замка)
5. Встановіть виносні зчитувачі та виконайте підведення їхніх кабелів
6. Виконайте підведення шлейфів від датчиків/кнопок
7. Виконайте підведення кабелю Ethernet
8. Виконайте укладання монтажних кабелів у стіні
9. Встановіть та закріпіть корпус контролера,
10. Виконайте комутацію дротів блоку живлення, замка, зчитувача, входів контролера зі шлейфами відповідно до розділів, наведених нижче
11. Здійсніть підключення кабелю Ethernet до гнізда
12. Закрийте кришку та зафіксуйте гвинтом
13. Підключіть у ПО СКУД контролер (відповідно до інструкції СКУД)
14. За допомогою СКУД виконайте повне завантаження (налаштування входів, виходів, розкладів, ідентифікаторів і т.д.) контролера.
15. Пристрій готовий до роботи

Рекомендації щодо монтажу

Розміщувати контролер слід у місці, доступному для обслуговування.

Для встановлення контролера на стіні необхідно виконати такі дії:

- відкрийте кришку корпусу, прикладіть корпус до передбачуваного місця кріплення та виконайте розмітку отворів;
- пропустіть дроти в отвори в стінці корпусу;
- закріпіть корпус контролера;
- виконайте підключення дротів.

Підключення зовнішнього зчитувача

Контролер має два порти з інтерфейсом Wiegand для підключення зчитувачів.

Разом з контролером можуть працювати різні зчитувачі.

На мал. 10 показаний приклад підключення зчитувачів

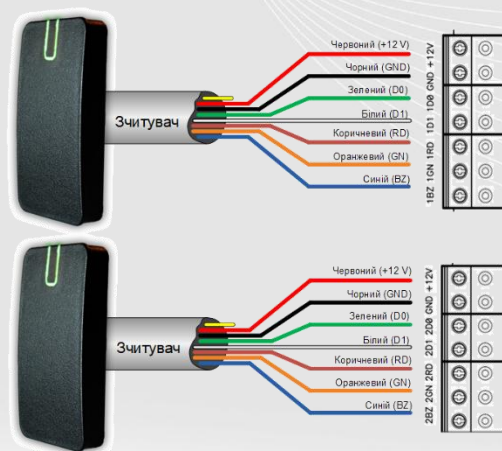


Рис.10. Підключення зчитувачів

Відповідність кольору дротів:

- білий - data 1
- зелений - data 0
- синій - включення бузера
- коричневий - увімкнення червоного індикатора
- помаранчевий - включення зеленого індикатора
- чорний - GND
- червоний - +12 V

При використанні зчитувачів різних виробників кольори дротів можуть відрізнятися. Відповідність кольорів дротів дивіться в інструкції з експлуатації на зчитувачі.

Струм споживання кожного зовнішнього зчитувача, що підключається до клем "+12V", не повинен перевищувати 100мА. При підключенні до контролера зчитувачів великої дальності зі струмом споживання понад 100 мА, напругу живлення на них необхідно подавати від окремого джерела.

Підключення шлейфів

Контролер має вісім входів для підключення шлейфів із контролем струму. Призначення кожного входу задається при програмуванні контролера. Можливі такі функції для входів:

- датчик проходу (дверний контакт)
- кнопка запиту на вихід
- датчик проходу (дверний контакт) + кнопка запиту на вихід
- вільний прохід (A, B, A+B)

- блокування (А, В, А+В)
- моніторинг стану датчика (тривожний датчик)

Нижче описано підключення різних типів входів. Після скидання контролера до заводських установок, всі шлейфи не мають призначення і не контролюються. Усі шлейфи працюють як на замикання, так і на розмикання. Використання навантажувальних резисторів є обов'язковим.

Нормальний стан шлейфу - від 1,4 кОм до 3 кОм, К.З. шлейфу – менше 1,4 кОм, розрив шлейфу – більше 3 кОм.

Кнопка запиту проходу

Кнопка запиту проходу застосовується, якщо прохід через двері контролюється тільки з одного боку. Відкриття дверей відбувається при натисканні та відпусканні кнопки запиту проходу.

Крім того, кнопка запиту проходу може використовуватись як кнопка дистанційного відкриття дверей. Наприклад, для відкриття дверей вручну секретарем чи охоронцем.

На мал. 11 показаний приклад використання підключення нормально розімкнених кнопок запиту на вихід для контактів Z1 і Z2.

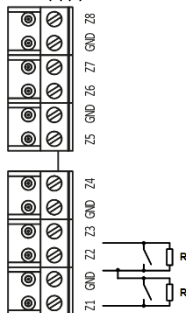


Рис.11. Підключення кнопки запиту проходу

При програмуванні призначено відповідність:

- Z1 – кнопка запиту проходу точки проходу А
- Z2 - кнопка запиту проходу точки проходу В

Використання для відкриття дверей кнопки на електрозамку або кнопки пропуску на пульті турнікету призводить до виникнення події ЗЛОМ ДВЕРЕЙ.

Для правильної роботи при програмуванні необхідно призначити підключені шлейфи, як шлейфи кнопки запиту проходу.

Датчик проходу (Дверний контакт)

За допомогою дверного контакту контролер визначає стан дверей (відчинені/зачинені) або положення ротора турнікету. У разі відсутності дверного контакту контролер не зможе виявити несанкціонований доступ або випадок, коли двері утримуються у відкритому стані надто довго (прохід кількох людей по одній перепустці).

На мал. 12 показаний приклад використання підключення дверних контактів (нормально закритих) входів Z3 та Z4:

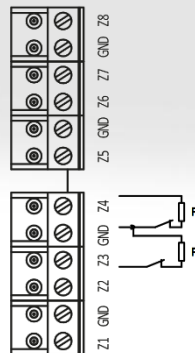


Рис.12. Підключення дверного контакту

При програмуванні призначено відповідність:

- Z3 – дверний контакт точки проходу А
- Z4 – дверний контакт точки проходу В

Двері, керовані системою контролю доступу, рекомендується обладнати доводчиком.

Для правильної роботи дверного контакту при програмуванні необхідно призначити підключені шлейфи як шлейфи дверного контакту.

Контролер може працювати без призначення дверного контакту. У такому разі, після піднесення ідентифікатора та надання доступу, генерується подія "Прохід відбувся", контролер подає відмикаючий імпульс на замок, і відраховується час проходу.

Комбінований шлейф – кнопка запиту на вихід та датчик проходу (дверний контакт)

Входи контролера можна налаштувати для одночасного використання кнопки запиту на вихід і для дверного контакту. При такому використанні розрив шлейфу означає порушення дверного контакту, а коротко - натискання кнопки запиту на вихід.

На мал. 13 показаний приклад використання підключення комбінованих шлейфів до входів Z5 та Z6:

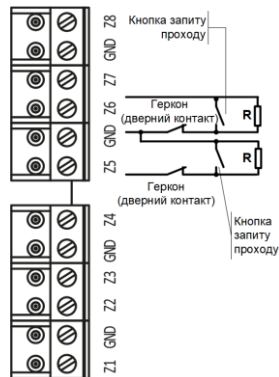


Рис.13. Підключення комбінованого шлейфу

При програмуванні призначено відповідність:

- Z5 - комбінований дверний контакт та кнопка запиту проходув точки проходув А
- Z6 - комбінований дверний контакт і кнопка запиту проходув точки проходув В

Будь-який із 8 входів може бути призначений як комбінований для обслуговування дверного контакту та кнопки запиту на вихід

Інтеграція з охоронно-пожежною сигналізацією

Завдяки наявності шлейфів, запрограмованих як ВІЛЬНИЙ ПРОХІД та БЛОКУВАННЯ, контролер повноцінно інтегрується в систему охоронно-пожежної сигналізації (див. мал. 14).

Для спільної роботи з пожежною сигналізацією необхідно запрограмувати будь-який шлейф на тип "Вільний прохід". До цього шлейфу може бути підключено безпосередньо пожежний шлейф або вихід пожежного ППК. При включенні пожежної тривоги порушується шлейф контролера, призначений як "Вільний прохід", всі двері керовані контролером автоматично розблокуються і персонал може вільно залишити зону пожежі.

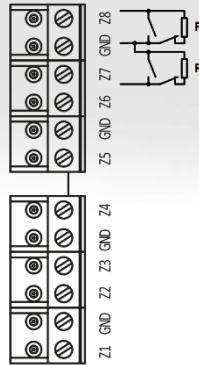


Рис.14. Підключення шлейфів блокування та вільного проходу

При програмуванні призначено відповідність:

- Z7 - "Блокування А+В"
- Z8 - "Вільний прохід А+В"

"Блокування" можна призначити на точки проходу А, В та А+В

"Вільний прохід" можна призначити на точки проходу А, В та А+В

Зони з типом **Блокування** та **Вільний прохід** спрацювають і КЗ і Обрив.

Для спільної роботи з охоронною сигналізацією необхідно запрограмувати будь-який шлейф на тип "Блокування". До цього шлейфу може бути підключено безпосередньо тривожний шлейф або вихід охоронного ППК. При спрацюванні охоронного датчика або включенні охоронної тривоги порушується шлейф контролера, призначений як "Блокування", і всі двері, керовані контролером, автоматично блокуються. При цьому доступ в приміщення, що охороняються, надаватиметься лише службі безпеки.

Виконавчі пристрої

Для управління виконавчими пристроями контролер має чотири реле. За допомогою виходів контролер може керувати електрозамком або засувкою, керувати роботою шлагбауму, турнікета, або включати інше додаткове обладнання.

Реле 1 і 2 мають нормально замкнуті та нормально розімкнені контакти. Контакти реле дозволяють керувати виконавчими механізмами зі струмом споживання до 1А при напрузі 24 ст.

Не допускається застосування діодів під час підключення виконавчих механізмів до електромережі змінного струму.

Викиди або провали напруги живлення при одночасному увімкненні-вимкненні всіх виконавчих пристроїв не повинні призводити до збоїв у роботі контролера. В іншому випадку необхідно підключити для живлення виконавчих пристроїв окреме джерело живлення.

Електрозамок

Наявність нормально закритих і нормально відкритих релейних контактів, а також можливість програмування часу спрацьовування замка в широких межах (від 1 до 255 секунд) дозволяє контролеру керувати електрозамками та засувками практично будь-якого типу.

Особливим випадком є час, що дорівнює 0. У цьому випадку на реле подається імпульс тривалістю 200 ms.

На мал. 15 показаний приклад підключення виконавчих пристроїв, перший відкривається подачею напруги, другий - зняттям.

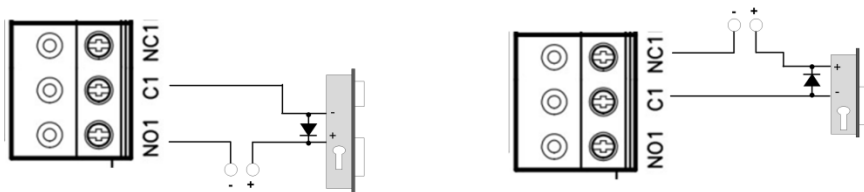


Рис.15. Підключення замків під час використання зовнішнього джерела живлення

При використанні контактів реле для увімкнення/вимкнення струму через індуктивне навантаження, наприклад, при керуванні електромагнітним замком, виникають електричні імпульси великої амплітуди. Для запобігання виходу з

ладу контактів реле необхідно шунтувати індуктивне навантаження діодом, включеним зустрічно напруги живлення котушки.

Слід враховувати, що недорогі електромагнітні засувки не допускають тривалої подачі напруги. Для таких засувок слід програмувати час реле таким, щоб не допустити перегрів котушки засувки.

Для правильної роботи замків, при програмуванні необхідно призначити підключені релейні виходи як виходи замків.

Сирени та дзвінки

Електродзвінки (див. мал. 16) для джерела напруги є індуктивним навантаженням, при підключенні дзвінка до джерела постійного струму необхідне використання захисного діода (дивись попередження про індуктивне навантаження).

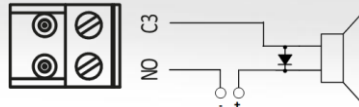


Рис.16. Підключення електродзвінків

При підключенні сирени вивчіть інструкцію користування сиреною. Струм споживання сирени не повинен бути більше 1 А.

При використанні нестандартних виконавчих пристроїв (магнітні пускачі, турнікети тощо) рекомендується за консультацією щодо підключення звернутися до свого постачальника обладнання.

Для правильної роботи сирени при програмуванні необхідно призначити підключений релейний вихід як вихід сирени (тривоги і т. д.).

Комунікація

Для зв'язку із сервером СКУД контролер U-PROX IP400 може використовувати дротову комп'ютерну мережу.

Налаштування приладу можливе автоконфігурацією або вручну з ПК за допомогою ПЗ "Конфігуратор".

При відповідному налаштуванні забезпечується:

- призначення статичної або динамічної (DHCP) IP адреси пристрою;
- робота з IP або DNS (доменним ім'ям комп'ютера) адресою сервера СКУД;

- Робота через мережу Інтернет (обслуговування віддалених філій) із можливістю резервування шляхів до Інтернету через другий маршрутизатор (роутер);

Контролер працює в автоматичному режимі - після завантаження даних з сервера виконує відпрацювання правил доступу для карток і надсилає повідомлення про це на сервер.

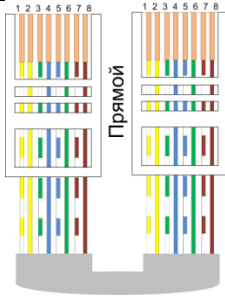
Комунікатор контролера працює в режимі **нотифікації**, тобто за наявності події (прохід, порушення зони) ініціюється передача даних на сервер СКУД.

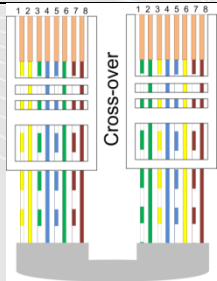
При роботі в комп'ютерній мережі контролер забезпечує захист від несанкціонованого втручання завдяки шифрування пакета даних з використанням 256-бітного ключа та контролю унікального серійного номера пристрою) а також контролю каналу зв'язку через періодичні тестові сигнали від пристрою.

Дротова комп'ютерна мережа (Ethernet)

Інтерфейс Ethernet використовується для об'єднання компонентів системи (ПК та контролерів) у мережу. Довжина кабелю Ethernet без додаткового обладнання може становити до 100 метрів, при цьому забезпечується швидкість передачі даних до 100Мбіт/с. На рис. 17 показано приклади підключення кабелю Ethernet.

Конектор 1	Конектор 2
Прямий обтиск, підключення до світчу або роутера	
1. біло-жовтий	1. біло-жовтий
2. жовтий	2. жовтий
3. біло-зелений	3. біло-зелений
4. синій	4. синій
5. біло-синій	5. біло-синій
6. зелений	6. зелений
7. біло-коричневий	7. біло-коричневий
8. коричневий	8. коричневий
Зворотній обтиск, підключення до комп'ютера	
1. біло-жовтий	1. біло-зелений
2. жовтий	2. зелений
3. біло-зелений	3. біло-жовтий
4. синій	4. синій
5. біло-синій	5. біло-синій
6. зелений	6. жовтий
7. біло-коричневий	7. біло-коричневий



8. коричневий	8. коричневий	 Мал.17. Підключення кабелю Ethernet
---------------	---------------	--

При налаштуванні Ethernet комунікатора контролера слід виконати:

- Налаштування параметрів мережі контролера (при використанні DHCP – не задаються):
 - IP адреса
 - Маска підмережі
 - IP адреса шлюзу (роутера) інтернет 1 (необов'язково в локальній мережі)
 - IP адреса шлюзу (роутера) в інтернет 2 (необов'язково)
 - IP-адреса DNS сервера 1 (якщо використовується передача даних на доменне ім'я)
 - IP-адреса DNS сервера 2 (необов'язково, якщо використовується передача даних на доменне ім'я)
- Налаштування комунікації з сервером:
 - IP або DNS адресу сервера 1
 - IP або DNS адресу сервера 2 (адреса U-PROX IC A)
 - Порти доступу (порт читання та порт запису)
 - Частота перевірки каналу зв'язку (надсилання тестового сигналу)

Порядок програмування контролера

Програмне забезпечення	Дії
	1. Визначення режиму роботи контролера: автономний або у складі СКУД
ПЗ "Конфігуратор" Через порт USB	2. Налаштування початкових параметрів, а саме мережевих налаштувань контролера: а. Налаштування сервера: IP-адреса або DNS ім'я сервера, порти доступу (порт читання, порт запису)

	Пункт d за наявності DHCP (динамічних адрес) у мережі не потрібно виконувати b. Установки пристрою: IP-адреса пристрою в комп'ютерній мережі, маска підмережі, IP DNS сервера, шлюз в Інтернет
ПЗ СКУД	3. Підключення та реєстрація пристрою в ПЗ СКУД (див. посібник зі СКУД) 4. Налаштування пристрою за допомогою СКУД - Налаштування дверей: односторонні двері або двосторонні двері, режим роботи Антидубль, час введення PIN-коду (або вимкнено) - Налаштування точок проходу: № зчитувача, час проходу, ознаки "Немає тривоги при зломі", "Немає тривоги, якщо відкрито занадто довго" - Налаштування зчитувачів: тип зчитувача 26 або 42 біт - Налаштування входів контролера: тип реакції та точка проходу (наприклад, датчик проходу, точка проходу А та В; вільний прохід, точка проходу В). - Налаштування виходів контролера: тип використання (замок, сирена і т.д.), режим роботи, тривалість імпульсу (якщо доступний у даному режимі), точка проходу, що управляє цим виходом. 5. Засобами СКУД створюється список користувачів з набором ідентифікаторів та їх додаткових параметрів, розклад правил проходу через певні точки проходу (див. посібник зі СКУД) 6. Після формування та завантаження конфігурації з ПЗ СКУД пристрій готовий до роботи.

Сервісне обслуговування

Скидання в заводські установки

Для повернення контролера до заводських установок слід виконати такі дії:

1. Відкрийте корпус контролера (поруште TMP)
2. Знеструмте контролер
3. Встановіть перемичку FACT
4. Подайте харчування

5. Зачекайте 40-50 секунд (або, якщо підключені зчитувачі, зачекайте на шість коротких сигналів, що сигналізують про успішне скидання контролера)
6. Знеструмте контролер
7. Зніміть перемичку FACT, закрийте корпус контролера (відновіть TMP)
- 8.

Перехід у режим програмування

Щоб перевести контролер у режим програмування, виконайте такі дії:

1. Не вимикаючи живлення, відкрийте корпус контролера (поруште TMP)
2. Підключіть до роз'єму USB кабель і виконайте налаштування приладу за допомогою програмного забезпечення "Конфігуратор"

Заміна мікропрограми пристрою

1. Відкрийте корпус контролера (поруште TMP)
2. Знеструмте контролер
3. Встановіть перемичку FACT
4. Підключіть USB кабель спочатку до комп'ютера, а потім – до контролера
5. За допомогою спеціального програмного забезпечення виконайте заміну мікропрограми контролера
6. Після завантаження програмного забезпечення в контролер обов'язково зачекайте 15-20 секунд (або, якщо підключені зчитувачі, дочекайтеся шести коротких сигналів, що сигналізують про завантаження мікропрограми) .

Увага! Завантаження мікропрограми буде дозволено лише протягом перших 10 секунд після запуску контролера.

Заводські налаштування

Комунікатор

DHCP увімкнена (не встановлено IP контролера), адреси сервера SKUД не вказані

Входи (шлейфи)

Z1 – Z8 – відключено

Виходи

Реле 1 – 4 - відключено

Зчитувачі

Wiegand 42bit

Технічне обслуговування та ремонт

Гарантійне та післягарантійне обслуговування контролерів U-PROX IP400 виконується особами чи організаціями, які отримали на це повноваження від виробника.

Гарантійні зобов'язання

Виробник гарантує відповідність контролера U-PROX IP400 описаним у даній інструкції параметрам протягом гарантійного терміну зберігання та гарантійного терміну експлуатації при виконанні умов зберігання та експлуатації, встановлених цим посібником з експлуатації.

Гарантійний термін зберігання – 6 місяців з дня виготовлення.

Гарантійний термін експлуатації – 24 місяців з моменту введення в експлуатацію.

Постачання приладів, навчання персоналу, монтаж, пусканалагоджувальні роботи та гарантійне обслуговування контролера U-PROX IP400 виконує виробник або організація, що отримали відповідні повноваження від виробника.

У разі проведення пусканалагоджувальних робіт організацією, що не має повноважень виробника на проведення цих робіт, споживач позбавляється гарантійного обслуговування.

Гарантійний ремонт не проводиться, якщо виріб вийшов з ладу у разі:

- неправильного підключення,
- недотримання вимог даного керівництва,
- механічних пошкоджень,
- стихійного лиха.

Фірма-виробник має право вносити до конструкції виробу зміни, що не впливають на основні технічні характеристики та надійність виробу.