U-Prox Access Control IP400 & U-Prox WEB – налаштування (швидкий старт)

Система дозволяє вирішувати завдання, пов'язані з контролем доступу в приміщення, на поверхи та багато іншого на будь-якому об'єкті: офіс, готель, банк, навчальний заклад, склад, фабрика та велике розподілене підприємство.

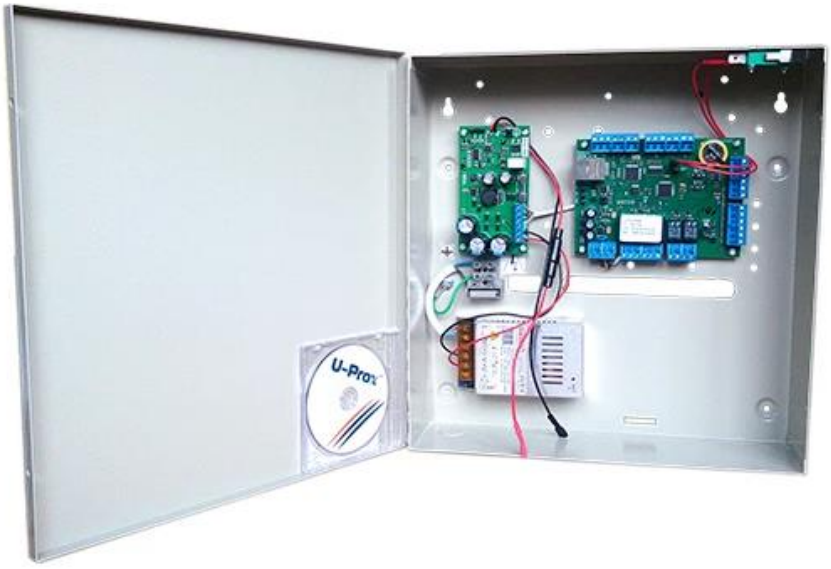
До мережевої СКД U-Prox Web входять: IP контролери, інтелектуальні зчитувачі, мобільні ідентифікатори та безкоштовне програмне забезпечення.

Тут ми детальне розглянемо стартове налаштування, характеристики, переваги та недоліки системи.

Ми розглянемо модель контролеру U-Prox IP400 з двоми зчитувачами. Серії інших контролерів, які ви можете подивитися на офіційному сайті зараз ми розглядати не будемо.

Таким чином почнемо, взявши універсальний IP контролер доступу U-Prox IP400 – це повнофункціональний пристрій із сучасними засобами комунікацій.

Це один з найбільш просунутих контролерів на ринку України, буває в двох варіантах - просто плата і плата в боксі (металевий ящик), з блоком живлення і місцем під акумулятор. Комплектація з боксом найзручніша, в ній ми розміщуємо акумулятор і отримуємо автономну систему, яка працює, навіть при зникненні електрики. Контролер відмінно обслуговує замок і не вимагає установки додаткових джерел живлення (якщо ви не купили максимальну комплектацію, до плати доведеться докупити джерело живлення). Для прикладу будемо використовувати варіант у металевому корпусі з блоком живлення 1.5А.



U-Prox IP400 може обслуговувати дві односторонні двері, тобто вхід за ідентифікатором, вихід за кнопкою виходу, або одні двосторонні двері – вхід та вихід проводиться за ідентифікатором в обох напрямках.

Працює він у IP мережах, підключається до мережі стандартним Ethernet кабелем, має роз'єм RJ-45, підтримує DNS, DHCP отримання IP адрес, може працювати зі складних

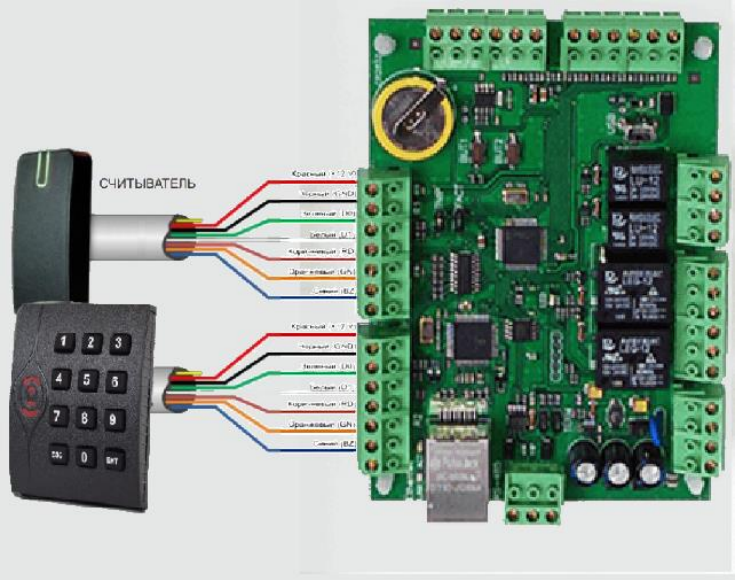
динамічно змінюваних комп'ютерних мереж, через численні NAT, включаючи мережу Internet, що робить його досить зручним пристроєм для побудови систем доступу.

Контролер не вимагає додаткових налаштувань мережевого обладнання, має розширену безпеку по роботі з IP, включаючи крипто- та емітостійкість протоколу.

Однак прилад розроблений з урахуванням максимальної автономності та за відсутності зв'язку з сервером він продовжує виконувати всі свої функції та завантажені до нього користувацькі дані та правила доступу.

Щодо інших характеристик, то не стану їх розписувати, а просто перерахую.

Як вже зрозуміло IP400 має два інтерфейси WIEGAND для підключення зчитувачів свого бренду, або сторонніх виробників. Наприклад, він підтримує ZKTeco.



Має місце у корпусі для встановлення резервного акумулятора, контакти та контролер його заряду з відповідною індикацією стану.

Підтримує 31700 шт. ідентифікаторів користувачів та 1000 тимчасових карток для відвідувачів, журнал на 47000 подій. Має енергонезалежну пам'ять на 250 часових зон, 250 робочих розкладів, 250 святкових та вихідних днів. Підтримує плаваючі розклади.

Для контролю та вхідної комунікацій з іншим обладнанням має 8 портів входів. Вони використовуються для підключення різних датчиків, кнопок виходу і таке наше. Якщо порти не використовуються вони мають бути заглушені резисторами.

Також контролер має 4 релейних виходи із сухим контактом: 2 виходу NO-NC та 2 виходу NC-NO.

Має конфігураційний роз'єм Mini USB для підключення до комп’ютера, до речи в пристрої доступна автоматична конфігурація, яку можна здійснити не через USB порт.

Тепер розглянемо те, без чого контролер лише груда залізяччя – розглянемо зчитувачі. До речі, вони заслуговують на особливу увагу.

Відмінна особливість зчитувачів U-Prox – це те, що вони є всеїдними тому, що можуть працювати у стандартах як Mifare, так EM-Marine, а ще підтримують mobile ID, що дозволяє

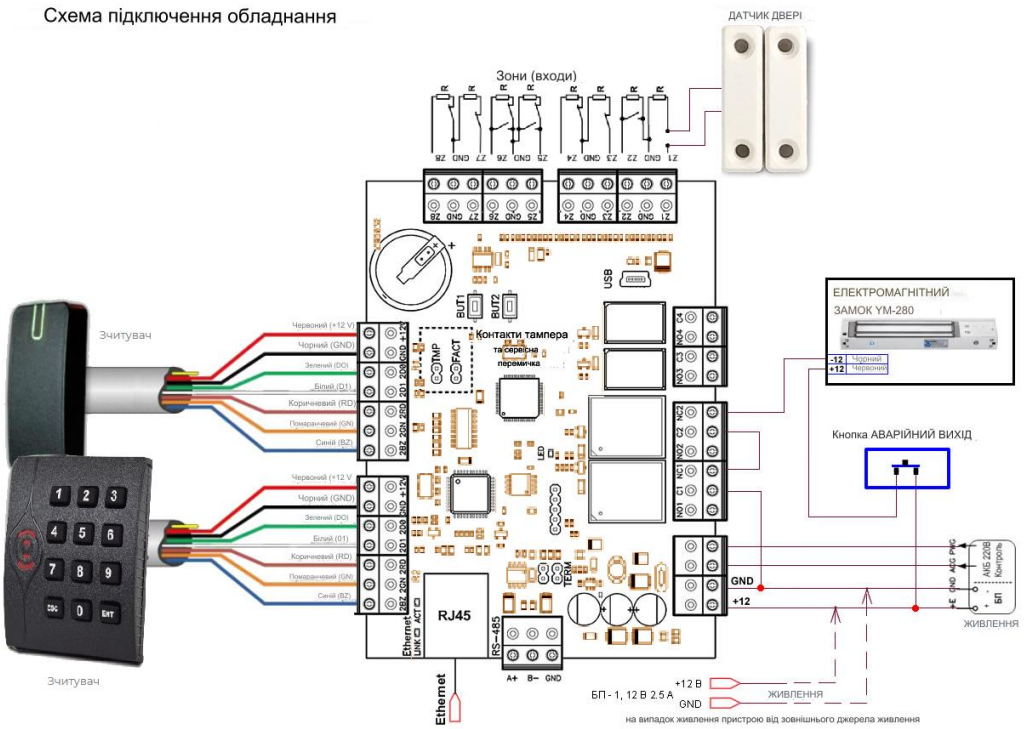
використовувати смартфон як карточку доступу, а також мають ось таких два зовнішні корпуси різних кольорів.

Також вони є універсальними і підходять під будь-яку іншу СКД завдяки WIEGAND інтерфейсу. Тобто ці зчитувачі U-Prox зовсім універсальні для будь-яких завдань і будь-яких контролерів, які ми можемо використовувати у себе на підприємстві.

Ну що ж з обладнанням U-Prox більш-менш розібралися, тепер спробуємо зібрати мінімально робочу схему.

Вже зрозуміло що для прикладу берем ці контролер та зчитувач, але зчитувачів буде 2. Один - рідний U-Prox Mini SL, другим для складності буде ZKTeco. Замок візьмем YLI YM-280. Підключили датчик дверей.

Тож ми зібрали схему и можемо переходити до налаштувань програмного забезпечення (ПЗ). Відразу зауважу одну особливість, справа в тому, що ПЗ стало абсолютно безкоштовним – без обмежень за ідентифікаторами, обладнанню та функціоналу.

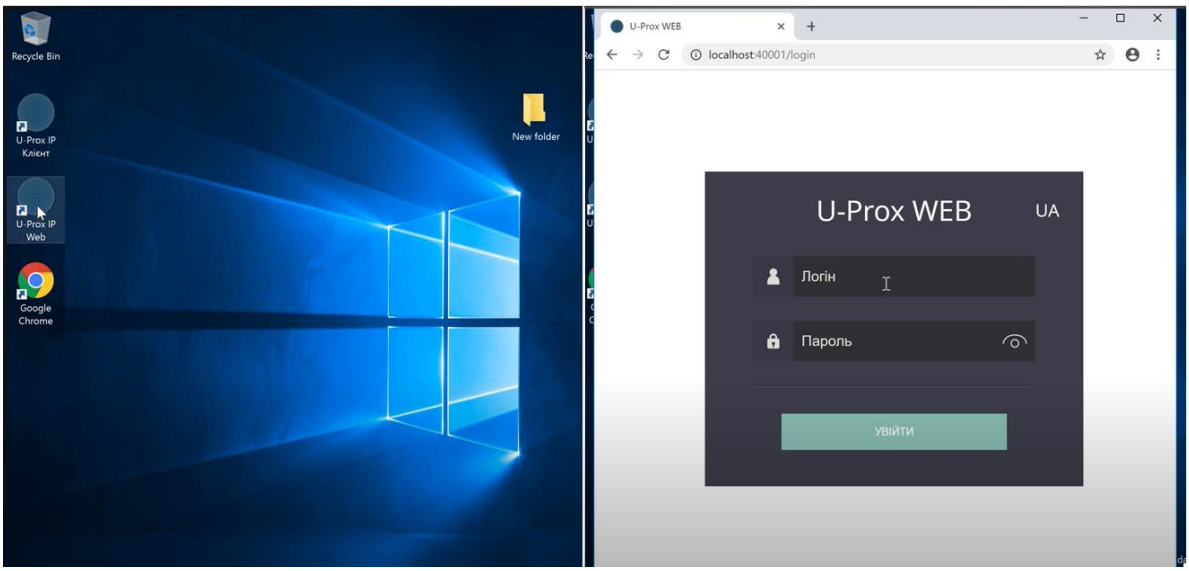


Розглянемо інтерфейс ПЗ, як він виглядає і яким буває, та що воно вміє, але для початку завантажмо його на свій комп'ютер. Скачати його можна з [офіційного сайту U-Prox]. На сьогодні доступна тільки одна опція: [U-Prox WEB. Образ DVD диска для встановлення/оновлення (ISO), 1070 Мб]. Її треба перенести на пустий DVD-диск, або використати ПЗ, яке створює з ISO образу віртуальний диск. До речі, у Windows 10 ISO-образ просто відкривається як папка, в якій можна відразу працювати з усіма файлами.

Раніше було дві версії: одна версія DESKTOP, а друга WEB, але тепер версія DESKTOP не підтримується виробником. Проте деякий період закачана раніше версія до ПК буде працювати, поки ні застаріє зовсім. Но ми не будемо її розглядати.

До речі, версія WEB дозволяє встановити наш сервер десь у хмарах і ні в чому собі не відмовляти, керуючи віддаленими об'єктами ну і отримуючи доступ природно з будь-якої точки світу.

Тож свіжу версію ПЗ ми встановили, налаштуємо її.



Після встановлення та запуску для доступу в програму необхідно ввести логін і пароль admin. Потім пароль треба змінити, оскільки безпека насамперед як-то кажуть.

Давайте розглянемо інтерфейс. Головна сторінка – меню, що відкриється пропонує функції системи, об'єднані в логічні групи – "Ролі". Необхідно вибрати роль фахівця і зайти в її робоче місце.

Робоче місце "**Адміністратор**". Має повнофункціональний інтерфейс для точного налаштування прав доступу системних операторів, управління дверима та оновлення програмно-апаратних засобів контролерів.

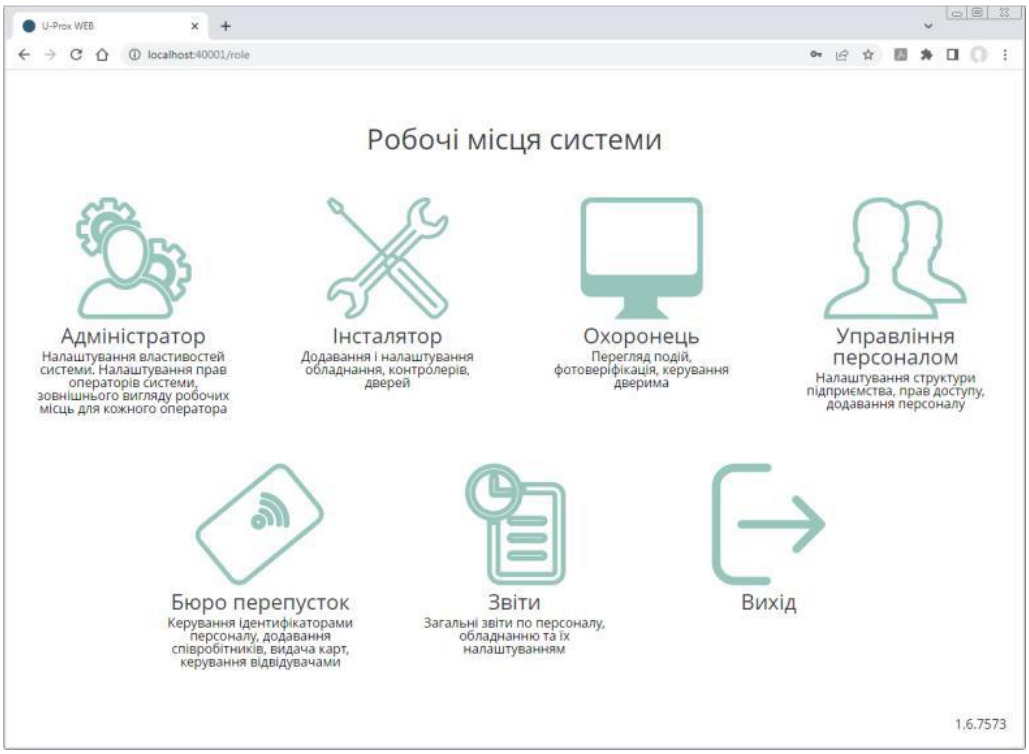
Робоче місце "**Інсталятор**". Дозволяє додавати в систему нові мережеві пристрої, відстежувати їх стан і версії вбудованого програмного забезпечення, налаштовувати двері, турнікети і ліфти і управляти ними.

Робоче місце "**Охоронець**". Дозволяє в режимі онлайн контролювати активність в системі, проводити фото-верифікацію. Це забезпечує можливість контролю дверей і їх розблокування в разі надзвичайної ситуації.

Робоче місце "**Управління персоналом**". Дозволяє налаштовувати структуру підприємства, створювати групи співробітників, надавати їм доступ в певні приміщення, видавати ідентифікатори і видаляти їх, формувати розклади як для груп співробітників, так і для конкретних осіб.

Робоче місце "**Бюро перепусток**". Дозволяє додавати і редагувати відділи, співробітників, працювати з ідентифікаторами, мобільними ідентифікаторами, деактивувати відвідувачів, здійснювати пошук співробітника за ідентифікатором і визначати його місце розташування.

Робоче місце "**Звіти**". Дозволяє формувати звіти про стан системи, події, персонал і відвідувачів, а також вести облік робочого часу.

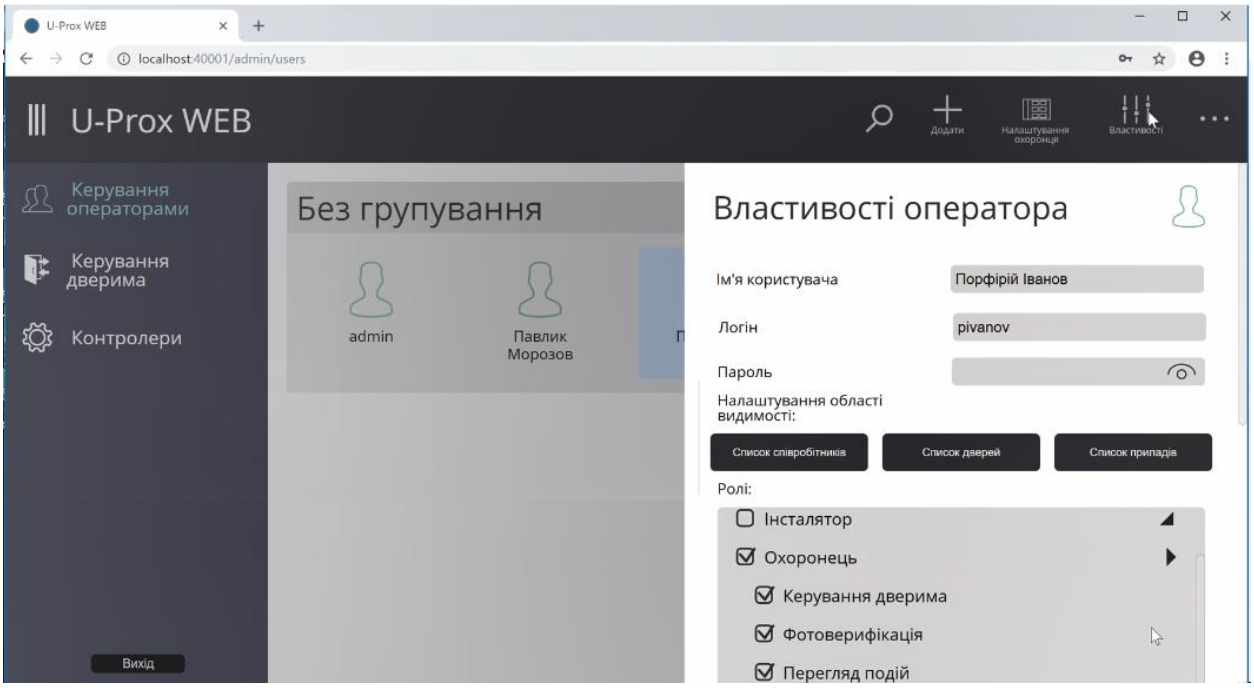


Як бачимо, інтерфейс найбарвистіший і найсучасніший, але повірте на слово, він досить практичний і згодом до нього звикаєш дуже швидко.

Спершу заходимо в робоче місце адміністратора і додаємо рольових користувачів-операторів. Для захисту системи від несанкціонованого втручання передбачена реєстрація операторів для входу в систему. Залежно від ролей та прав доступу, встановлених Адміністратором системи, оператори отримують доступ до різних функцій системи. Нам обов'язково будуть потрібні інсталятор, охоронець, управління персоналом і бюро перепусток, щоб правильно ввести контролер і вказати двері, а також додати користувачів з персоналу. На інші ролі та в якості звичайних робітників можна буде призначити користувачів пізніше.
Вважаю за потрібне згадати вже тут, що оператори не є персонал в звичному сенсі та їм не надається право на прохід, як і персоналу не надається можливість налаштування системи, а тільки доступ на прохід тими чи іншими дверима. Це абсолютно різні ролі в системі.

Отже почнемо. Виберіть в меню 

(див. малюнок нижче), щоб додати оператора системи. У вікні, введіть ім'я користувача, логін для входу в систему, пароль і повтор пароля. Далі оберіть ролі оператора та функції ролей до яких оператор матиме доступ. Наприклад, якщо вимкнути функцію "Керування дверима" оператору в ролі "Охоронець", то він зможе лише переглядати журнал подій та вікно фотоверифікації, також зможе керувати дверима, тільки якщо обрати й це.



Завивши користувачів, натискаємо кнопку" Вихід", і, підтвердивши дію, знову заходимо в програму за даними інсталятора, переходячи до додавання контролера.

Цей розділ слід переглянути насамперед після введення спеціальних операторів, необхідних для роботи самої системи. Для коректної роботи з обладнанням необхідно додати контролери, двері, та вказати – до яких контролерів які двері підключені, їх тип (односторонні, двосторонні) та параметри.

Для кожних дверей слід задати схему підключення виконавчих пристроїв. Схема підключення визначає тип вхідного та вихідного замка дверей, час його включення, а також режими використання шлейфів та виходів.

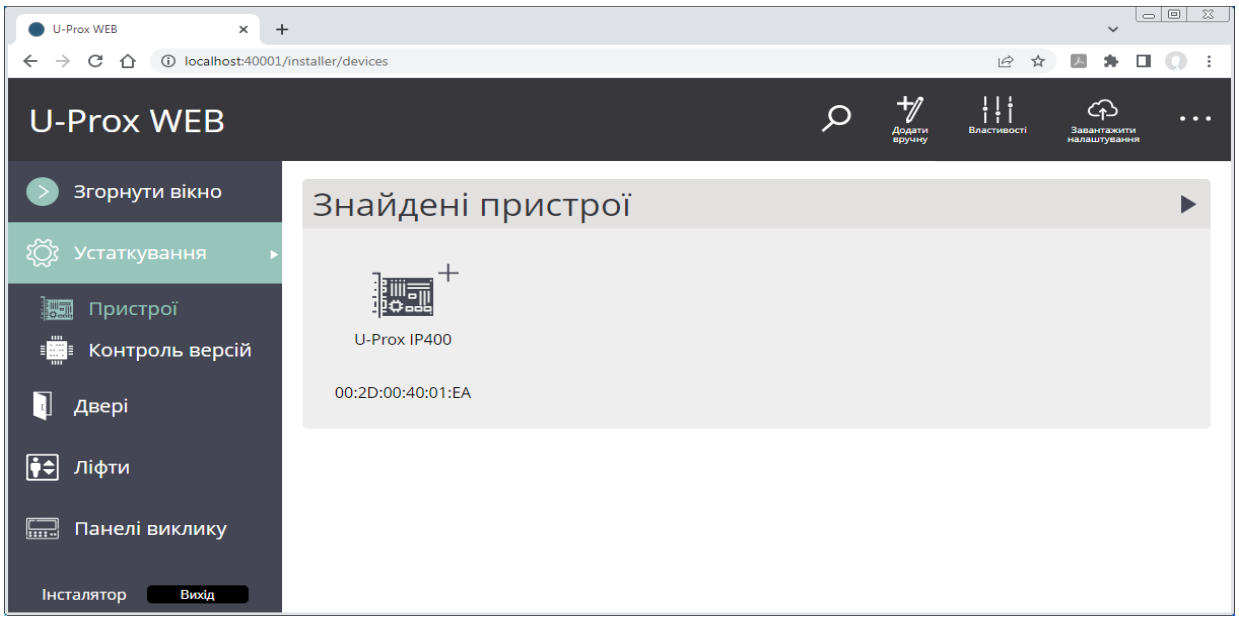
Перейдіть в розділ "Пристрої" (ліворуч на панелі). Додати обладнання можна двома способами – автоматично, ПЗ виконує пошук в локальній мережі, або вручну, вказавши тип пристрою та його серійний номер.

Система миттєво знайшла наш контролер – U-Prox IP400 з серійним номером.

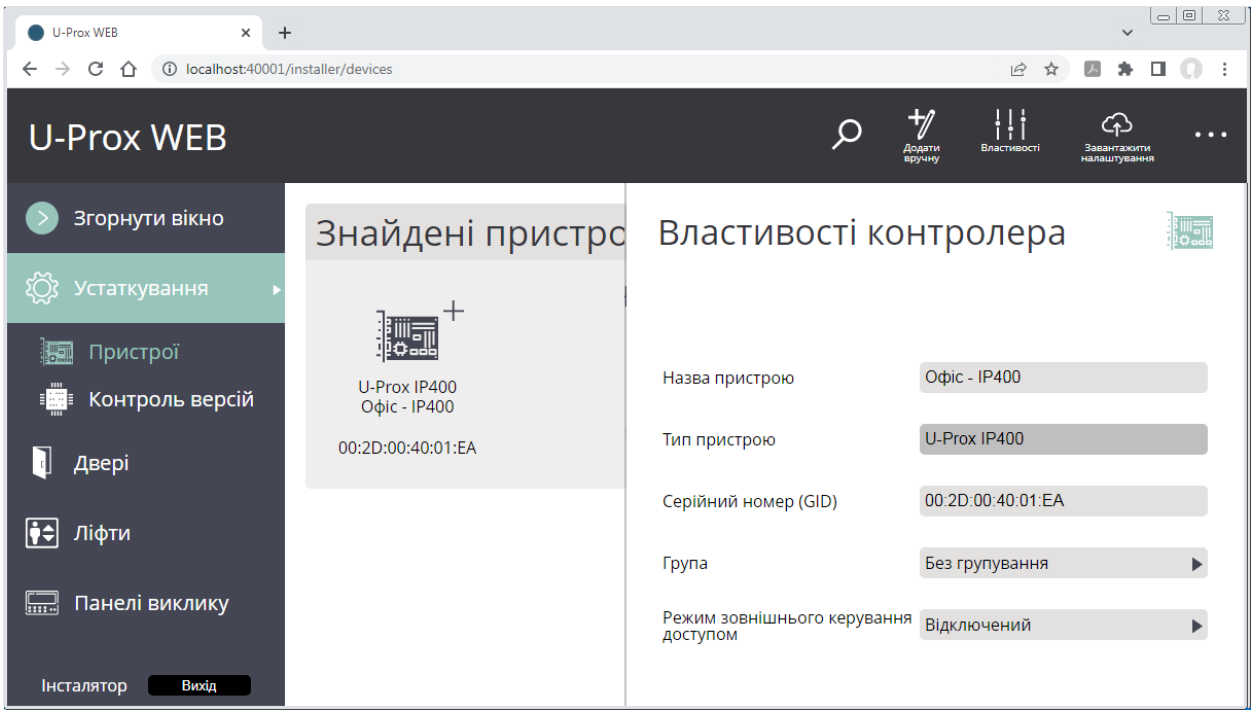
Все обладнання що є в підмережі сервера ПЗ U-Prox, і яке ще не було додано в базу, відображається в меню "Знайдені пристрої".

Щоб додати пристрій в базу – виберіть пункт меню "Властивості" 

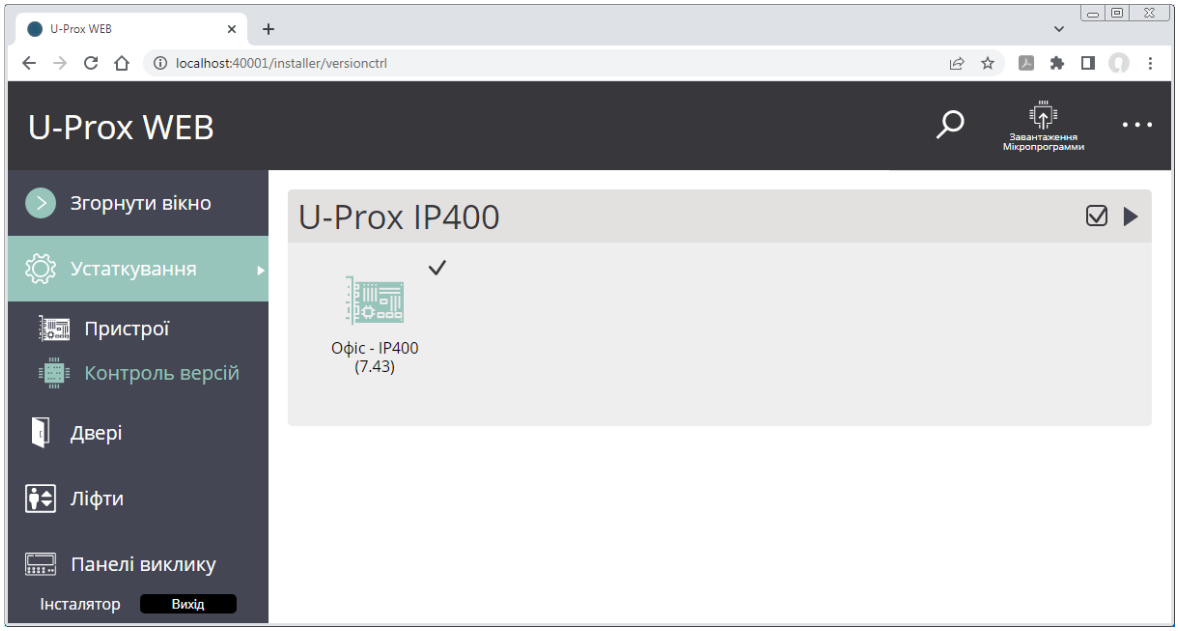
, чи натисніть  над іконкою (чи по самій іконці) знайдених автоматично контролерів:



Буде відкрито панель властивостей контролера:

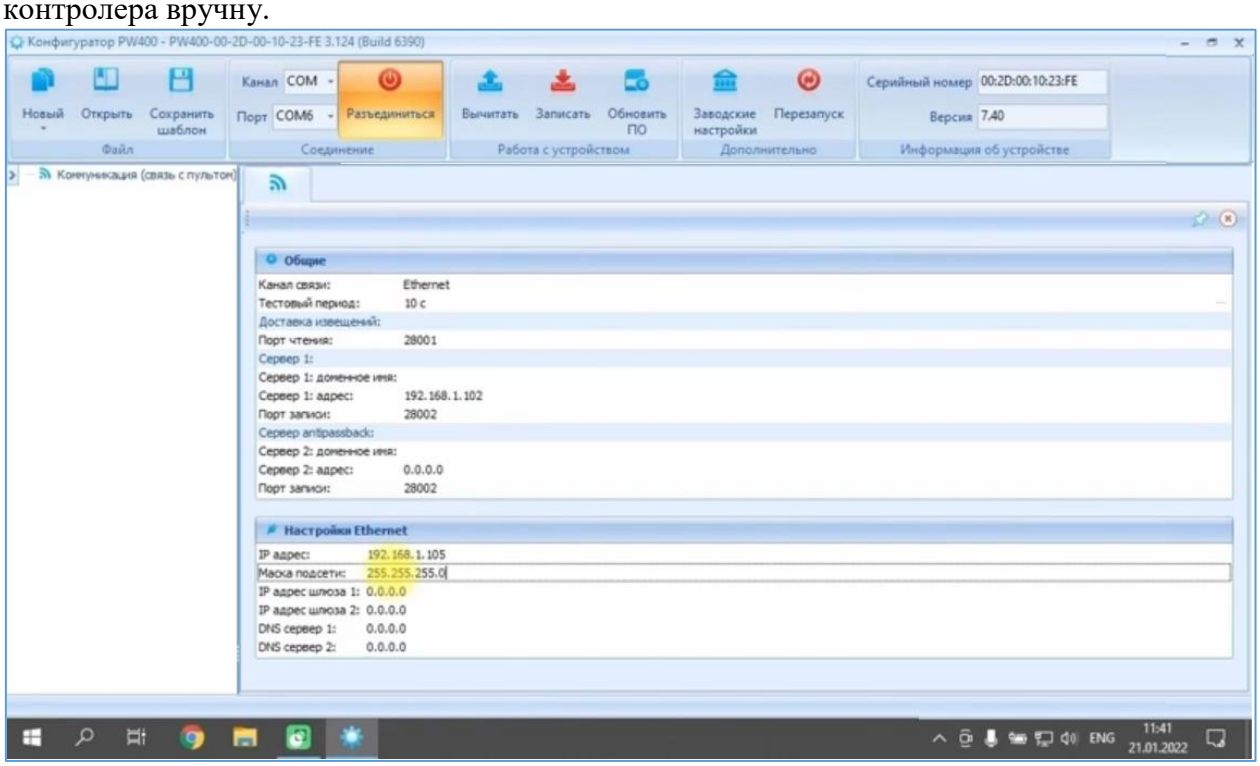


Введіть назву пристрою. Натисніть "OK", щоб зберегти зміни.



І ми бачимо, що контролер додався.

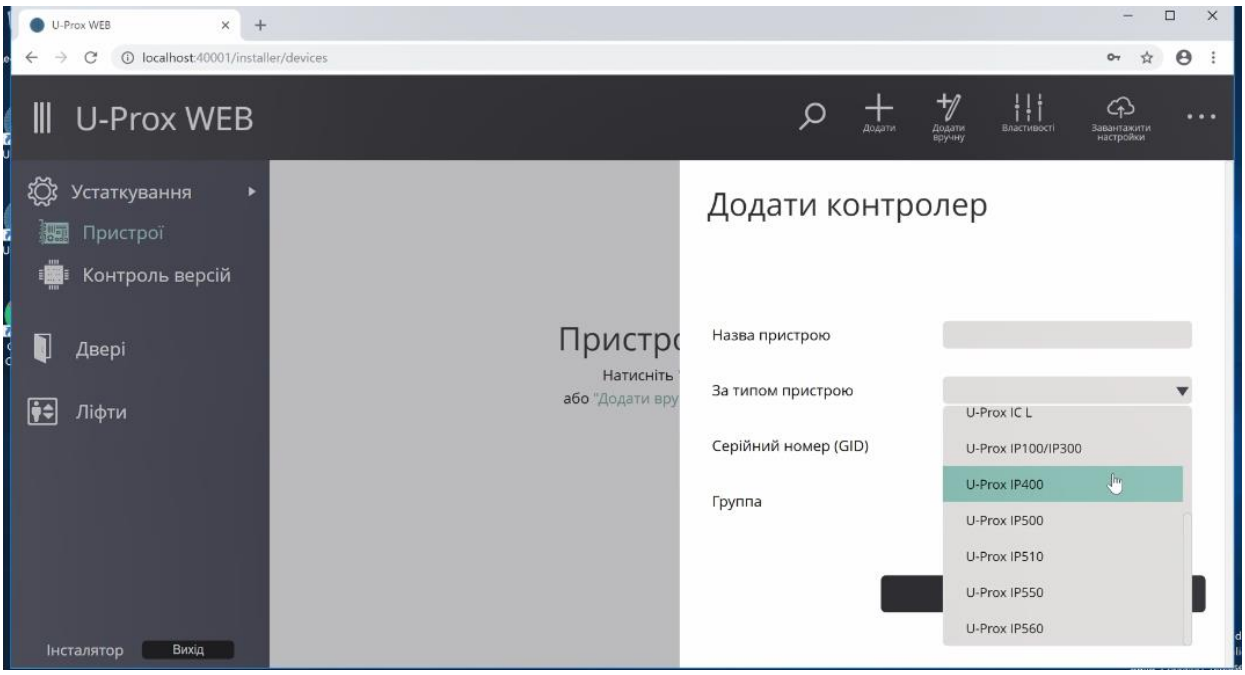
Якби ми встановили ПЗ не в тій же підмережі, в якій підключили контролер, але в ній не було б DHCP, то нам би довелося спочатку конфігурувати сам контролер за допомогою утиліти, вказуючи IP адресу, маску, DNS, якщо потрібно, а то і попередньо встановлювати драйвера USB, так як програма конфігуратор працює по шнурку,(до речі, незабуті зняти перемичку TEMP на час програмування), а потім вже в цій програмі вносити дані контролера вручну.



Цю програму та драйвер USB також можна завантажити з офіціального сайту виробника.

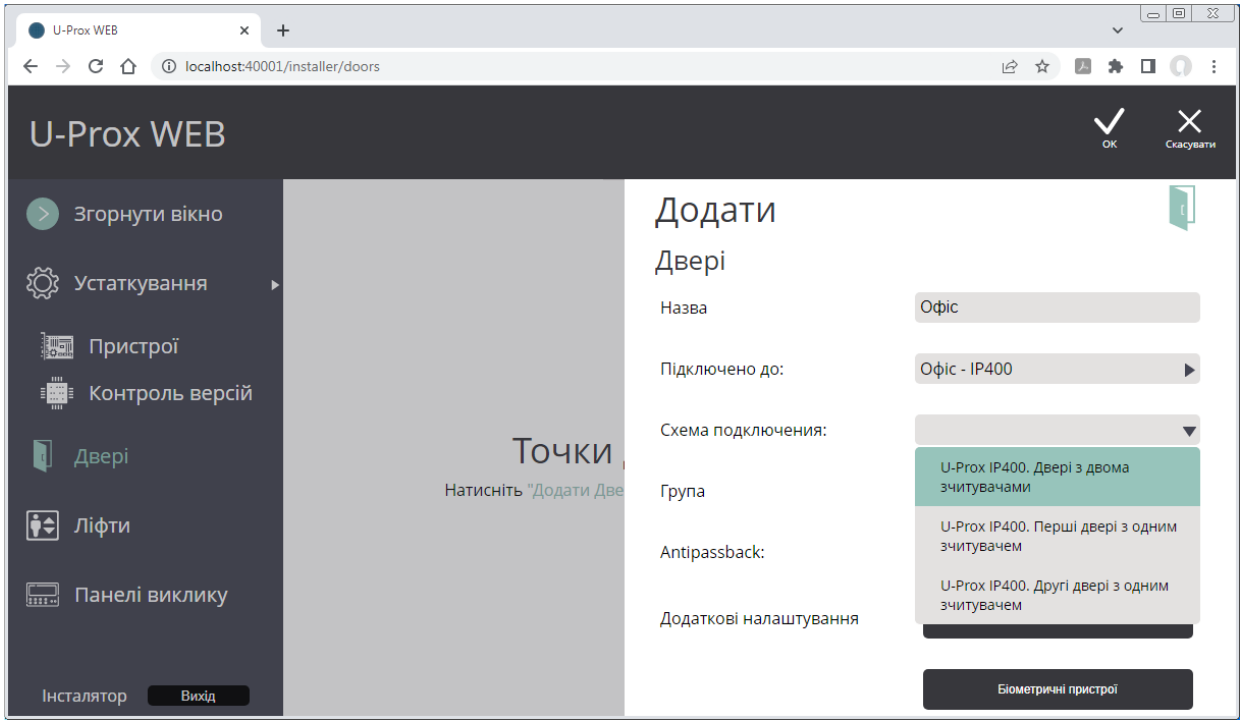
Щоб додати пристрій вручну, виберіть пункт меню "Додати вручну" 

, відкриється вікно параметрів нового контролера. Введіть назву пристрою, виберіть тип контролера, введіть серійний номер, додайте/виберіть групування пристрою. Натисніть "OK", щоб зберегти зміни.

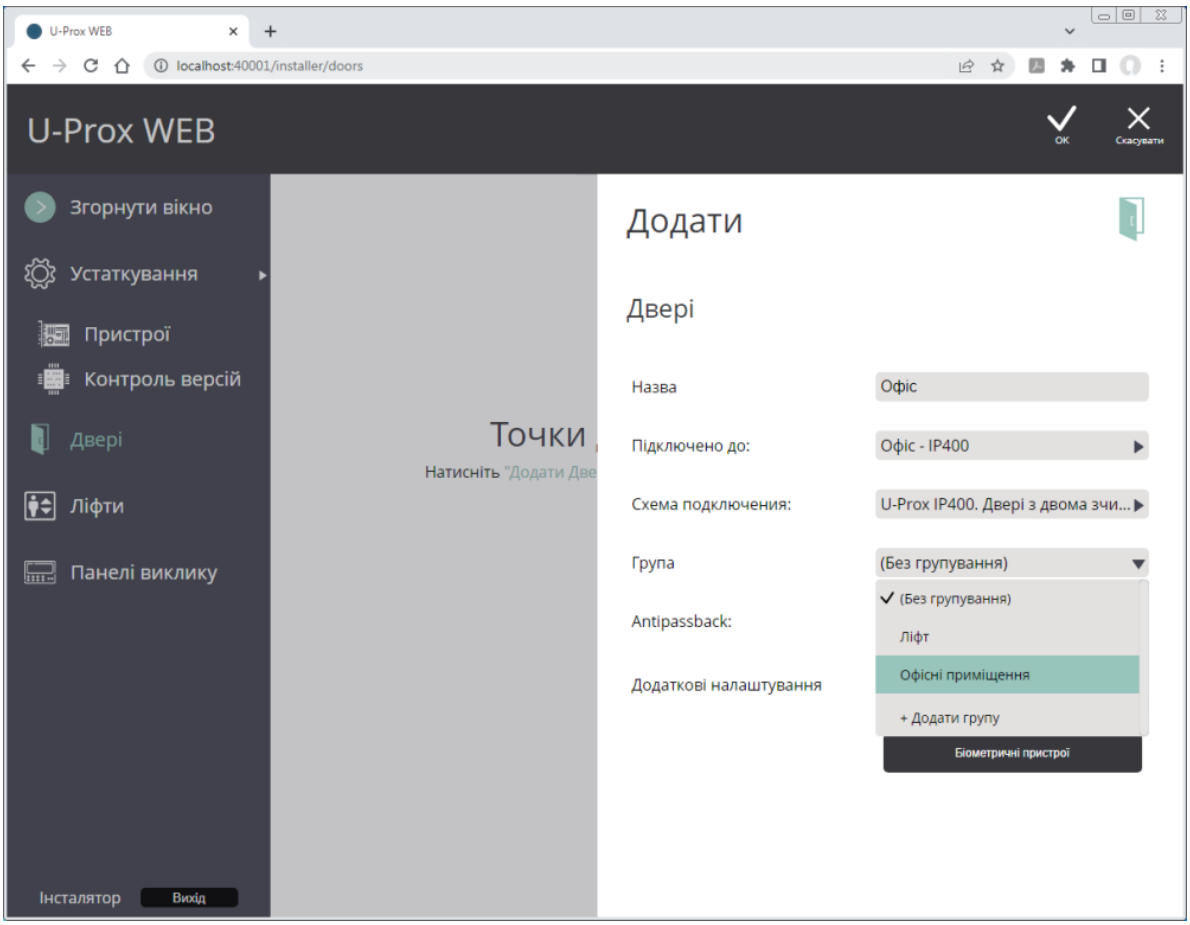


Побачивши, що контролер додався, його потрібно налаштувати. В першу чергу ми створюємо "Двері".

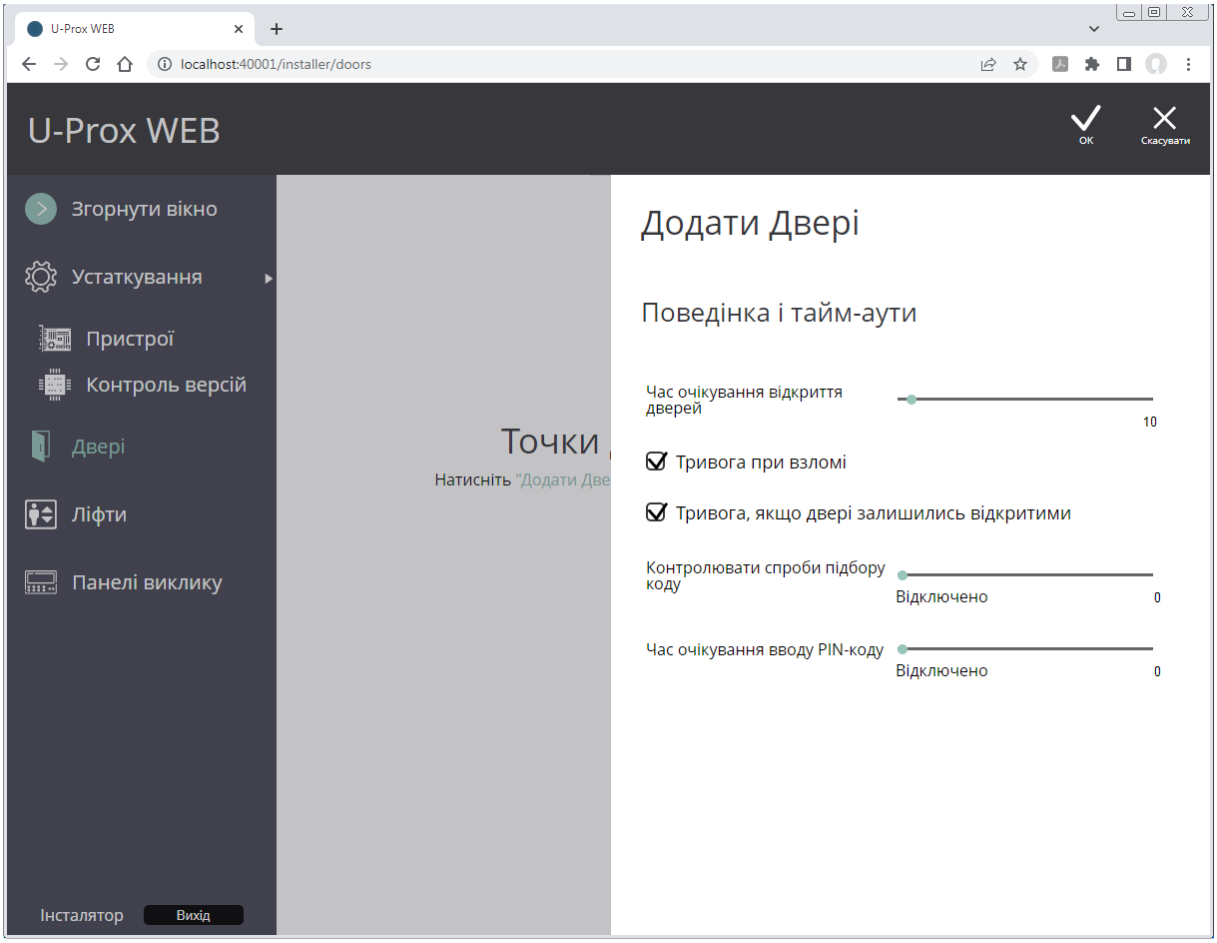
Для додавання дверей перейдіть до розділу "Двері" (ліворуч на панелі). Натисніть кнопку Додати. Вкажіть назву, виберіть пристрій, до якого будуть підключені елементи цих дверей. Далі стають доступними для вибору схеми підключення. Вони визначають типи реакцій входів, режими роботи виходів контролера, та роботу антидублю (antipassback, заборона повторного проходу).



Додайте створені двері до груп. Групи призначені для опису структурних одиниць об'єкта, наприклад група "Перший поверх", "Другий поверх" і т.і.



Надалі назву групи можна буде змінити.



Щоб змінити параметри дверей за замовчуванням, натисніть кнопку "Поведінка і тайм-аути". У вікні можна встановити наступні параметри:

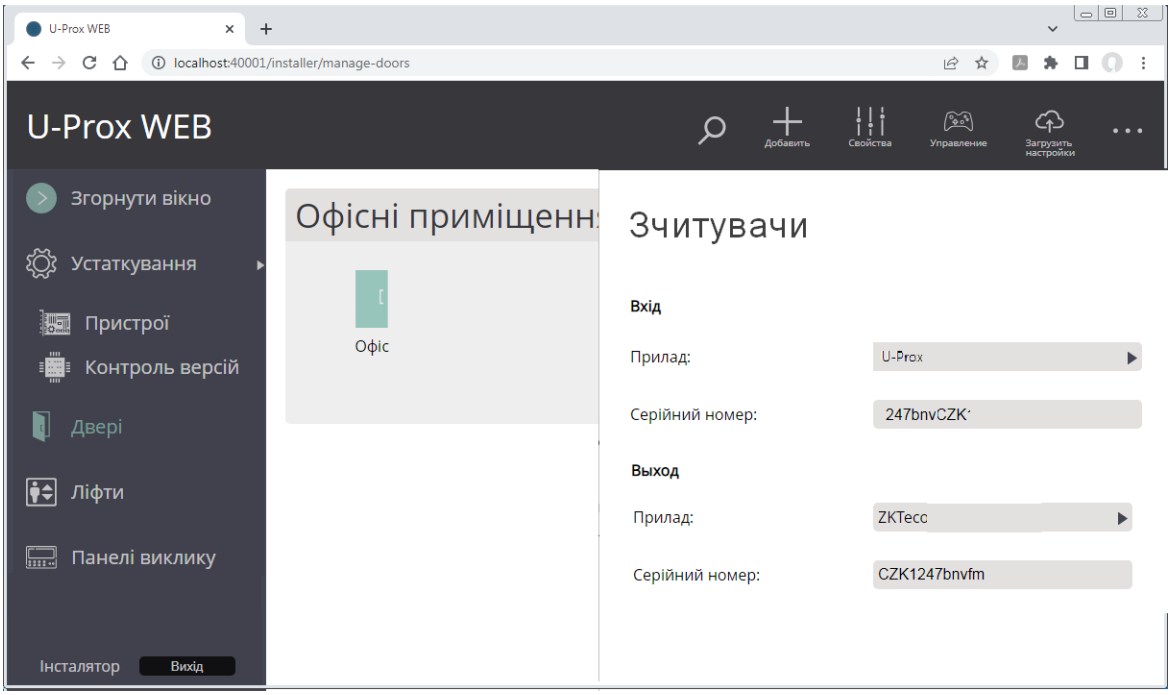
Час очікування відкриття дверей (час проходу) – час, протягом якого при дозволеному доступі двері повинні відчинитися і потім зачинитися. Це визначається порушенням та подальшим відновленням датчика проходу.
Тривога при зломі – при вимкненій опції двері та контролер не переходитимуть у стан "Тривога", якщо датчик проходу був несанкціоноване порушений.

Тривога, якщо двері залишились відчиненими – при вимкненій опції двері та контролер не переходитимуть у стан "Тривога", якщо двері були відчинені занадто довго (датчик проходу залишався порушеним після закінчення часу проходу).
Контролювати спроби підбору коду – кількість невідомих кодів (карток), введених підряд за невеликий відрізок часу, при перевищенні якого контролер переходить у стан "Тривога".
Час очікування вводу PIN-коду – кожен напрям проходу може бути оснащений зчитувачем з клавіатурою для введення PIN-кодів. Для того, щоб увійти через такі двері, необхідно не лише піднести картку до зчитувача, а й ввести цей код.
Щоб увімкнути контроль PIN-коду, встановіть достатній час очікування, наприклад – 15 секунд. Щоб вимкнути контроль, встановіть час 0 секунд.

Встановимо 3 перших параметри, щоб перевірити датчик дверей. Час відкриття дверей нехай буде 10 секунд, ставимо птички на тривоги.

Натисніть "OK", щоб зберегти зміни.

Все, ми бачимо що наші двері з'явилася в контролері. Тепер налаштуємо наші входи та виходи – можна привласнити який зчитувач у нас буде на вхід, нехай буде зчитувач номер 1 від U-prox, і на вихід зчитувач номер 2 від ZKTeco.

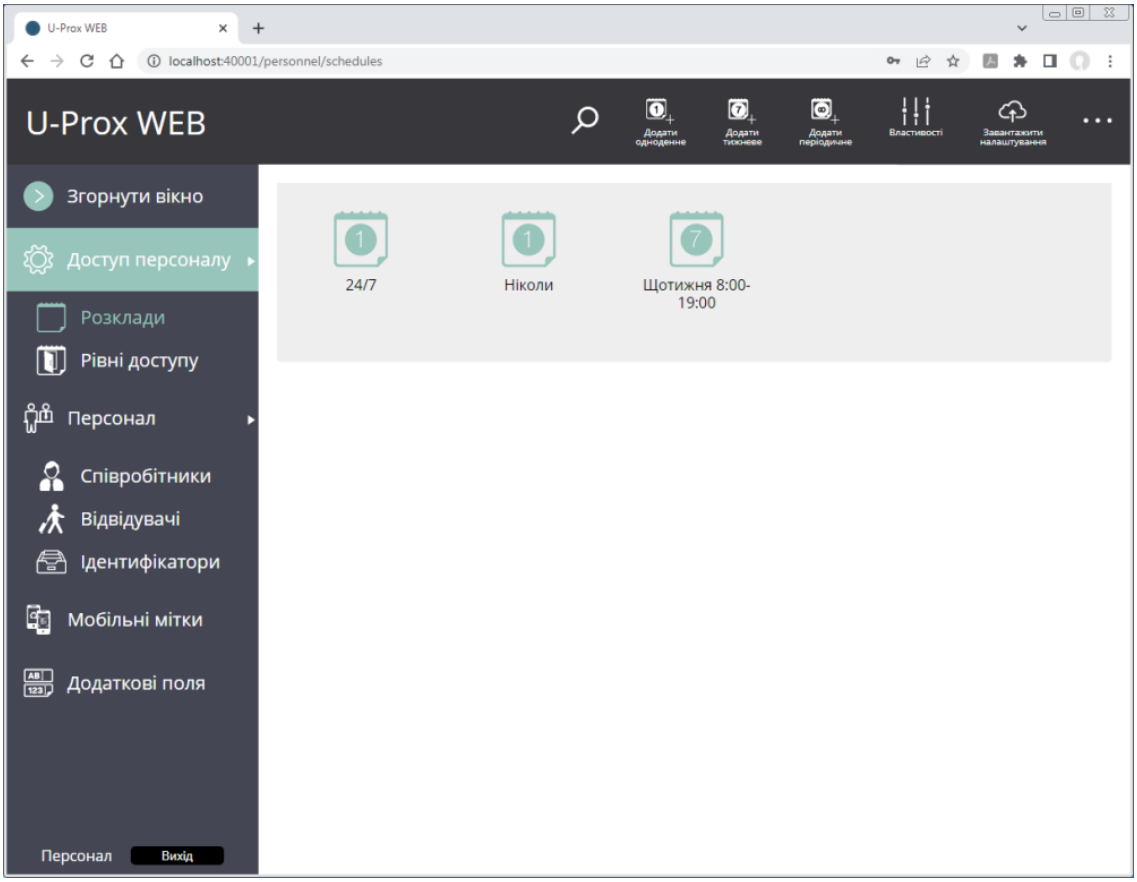


У двосторонніх дверях можна задати відповідності входу і виходу першому і другому зчитувачам, що може знадобитися для обліку робочого часу

Завивши двері та їх параметри, натискаємо кнопку "Вихід", і, підтвердивши дію, знову заходимо в програму за даними ролі Персонал, переходячи до додавання розкладів доступу, відділів та персоналу.

Задавати та відстежувати груповий доступ набагато зручніше, ніж індивідуальний. Тому перше, що потрібно зробити, це додати розклади, потім правила для рівнів доступу та внести в базу даних ієрархію персоналу. Для цього складіть список відділів, цехів та інших груп із вказанням до складу якого відділу чи цеху входить кожна група. Потім, по черзі, починаючи з найвищого рівня, додайте всі групи та відділи.

Важливий елемент правила доступу – розклад, адже саме за ним контролер визначає, коли можна пропускати співробітника, а коли не можна.
Система підтримує періодичні розклади із довільною довжиною періоду. Це можуть бути одноденні або семиденні тижневі розклади, а можуть бути і чотириденні, наприклад, доба-через-три.
Після встановлення системи користувачеві вже доступні три стандартні розклади – цілодобово "24/7", "Ніколи", та "Тижневе 8:00-19:00 (Пн – Нд)".
Щоб додати розклад, перейдіть до розділу "Розклади" (ліворуч на панелі). Натисніть відповідну кнопку "Додати одноденне", "Додати тижневе", "Додати періодичне".



Щоб змінити розклад, виділіть його √ і натисніть кнопку "Властивості" – відкриється вікно редагування.

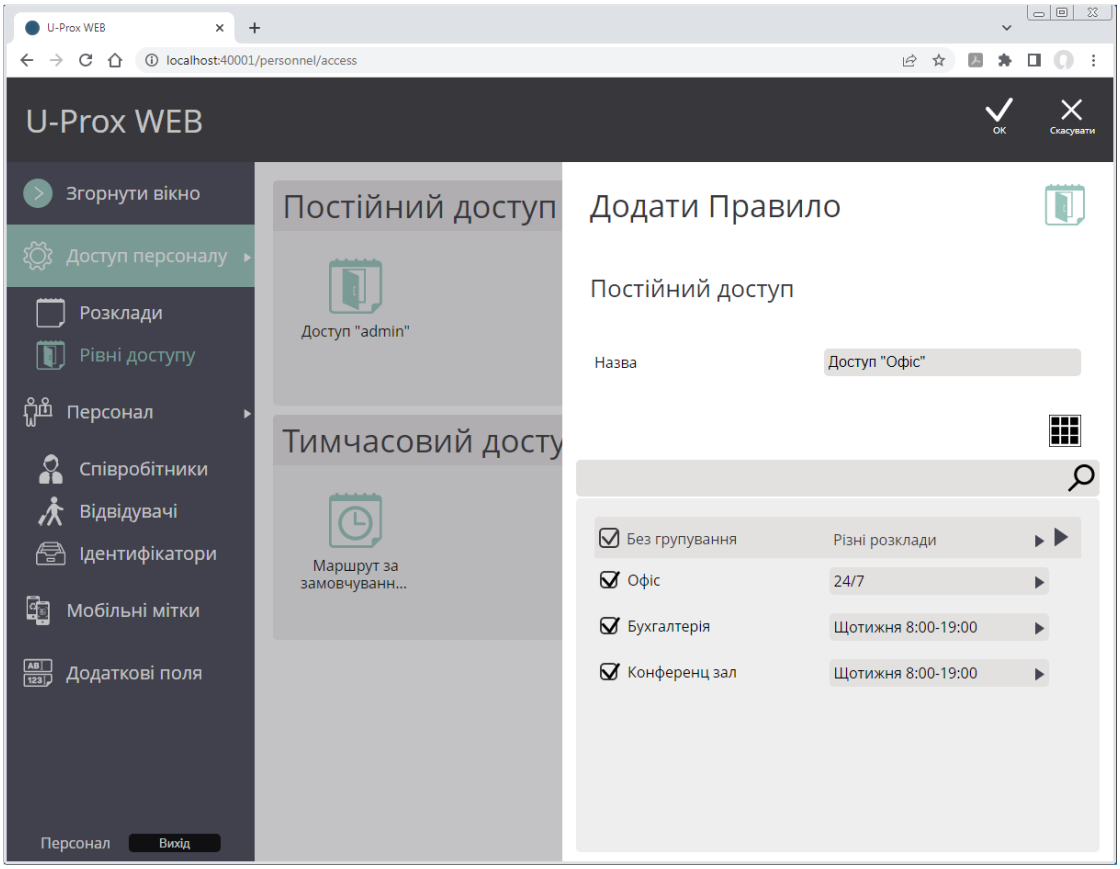
Після зміни параметрів існуючих розкладів – необхідно завантажити контролери. Для цього натисніть кнопку "Завантажити налаштування".

Але у нашому випадку змінювати розклади ми не будемо та скористаємся існуючими. Тому перейдемо до пункту «Рівні доступу».

Рівні доступу – правила, за якими контролер визначає, коли, і в які двері, можна пропускати співробітника, а коли не можна. Рівні доступу можуть бути призначені співробітнику та відділу співробітників, а також успадковуватись співробітниками від відділу в якому вони знаходяться.

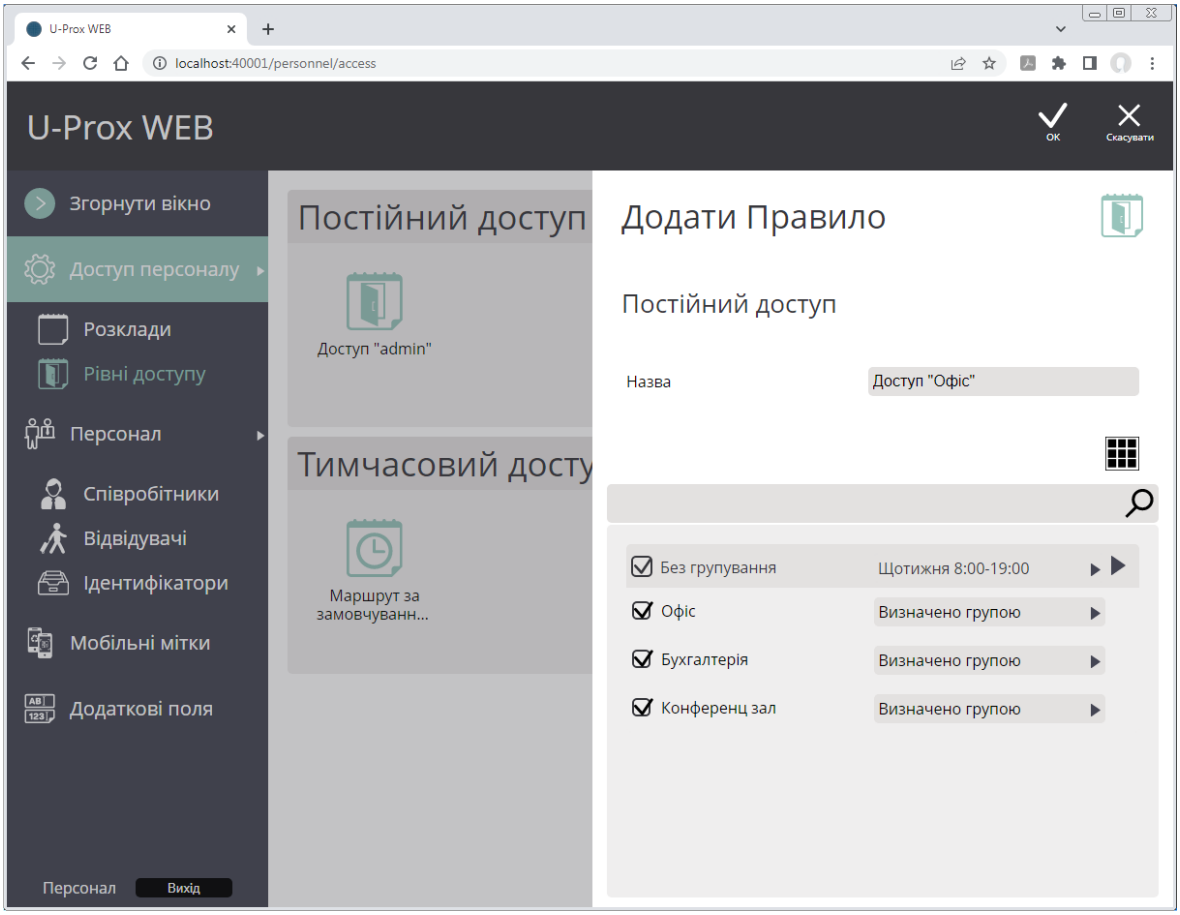
Існують два типи рівнів доступу – постійний, для співробітників, та тимчасовий, для відвідувачів.

Щоб додати доступ для співробітників, перейдіть до розділу "Рівні доступу" (зліва на панелі). Натисніть кнопку "Додати Рівень доступу", щоб додати постійний доступ.

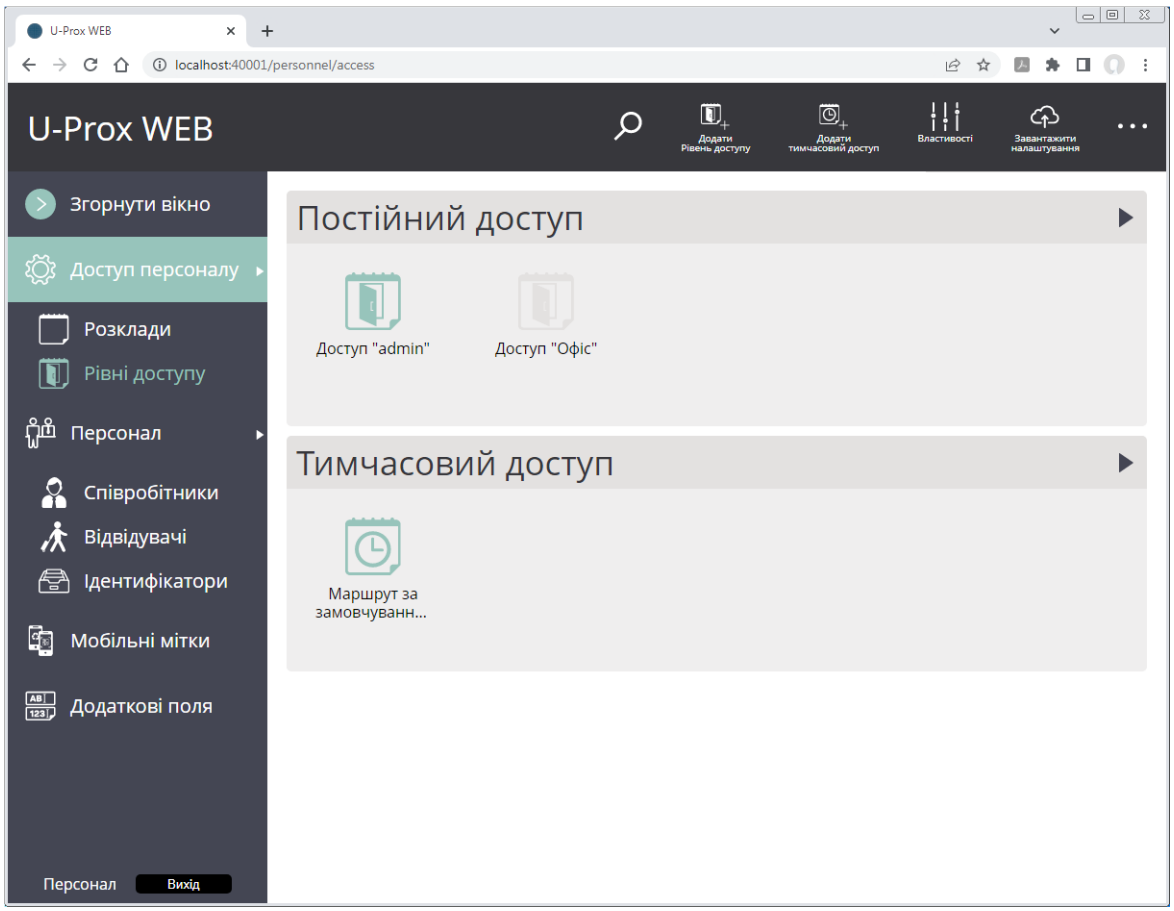


У вікні вкажіть назву правила, а також дозволені двері, встановивши коло них ☑, та виберіть розклад.

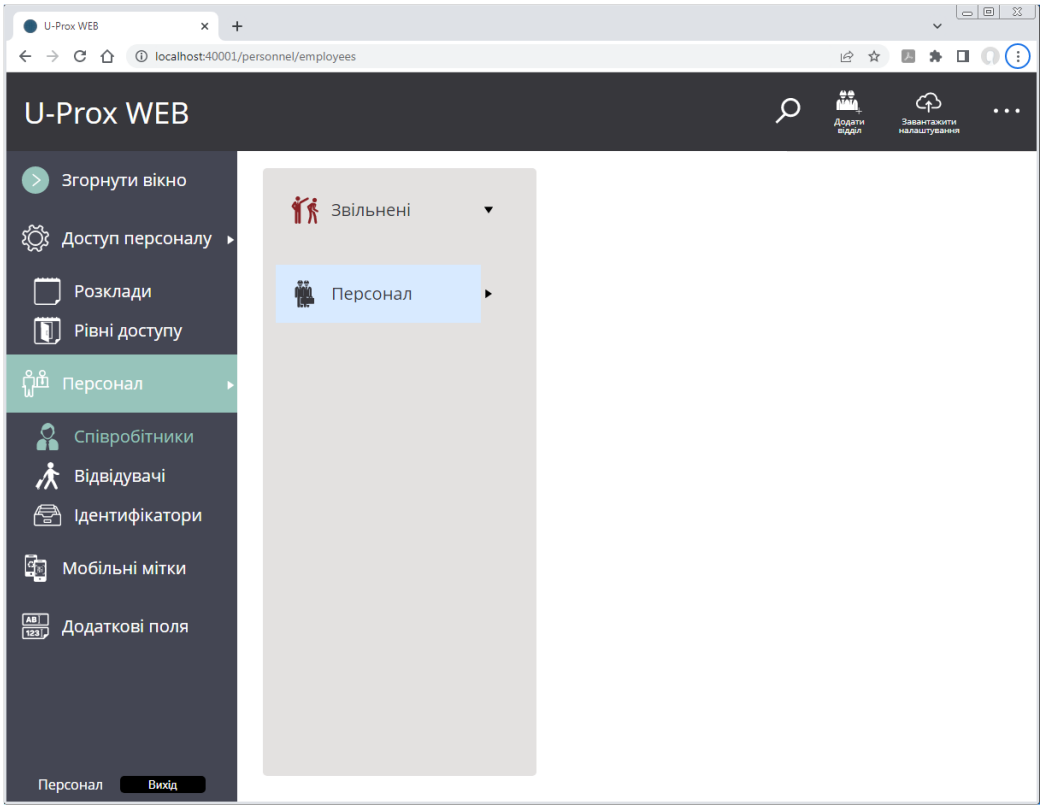
Якщо двері об'єднані у групу, то задавати їм усім розклад також можна групою.



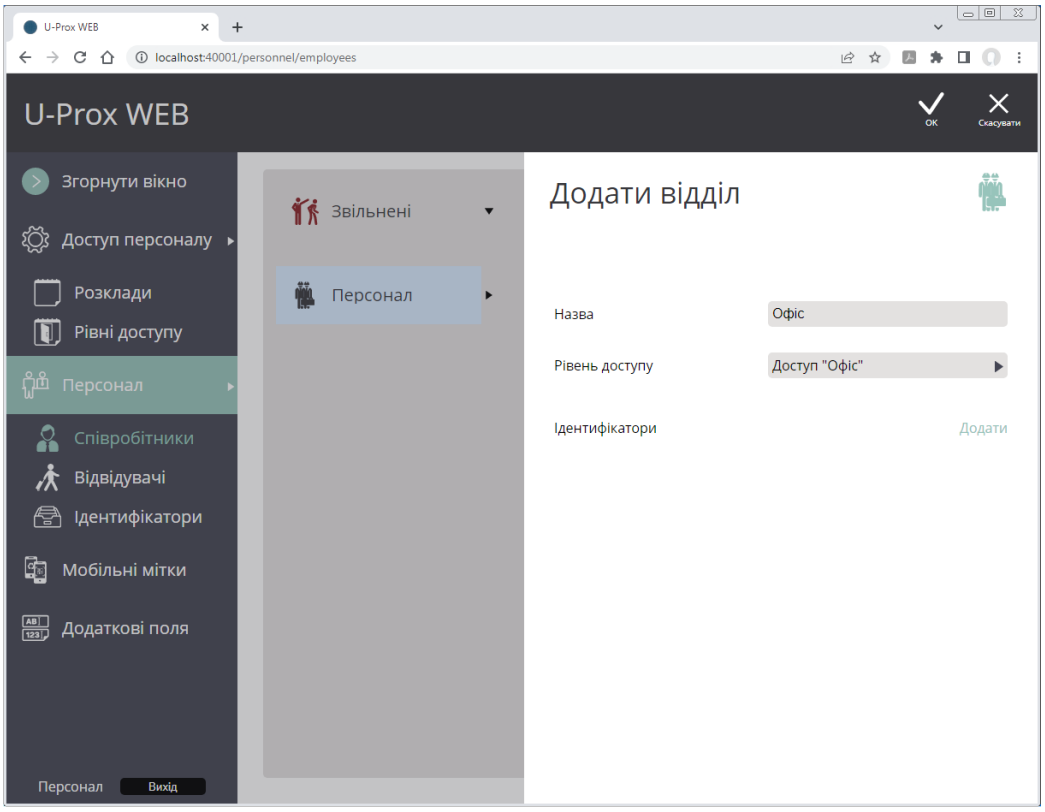
Буде створено рівень доступу. Якщо він ще не призначений жодному співробітнику чи відділу співробітників, то він матиме сірий колір, і буде можливе його видалення.



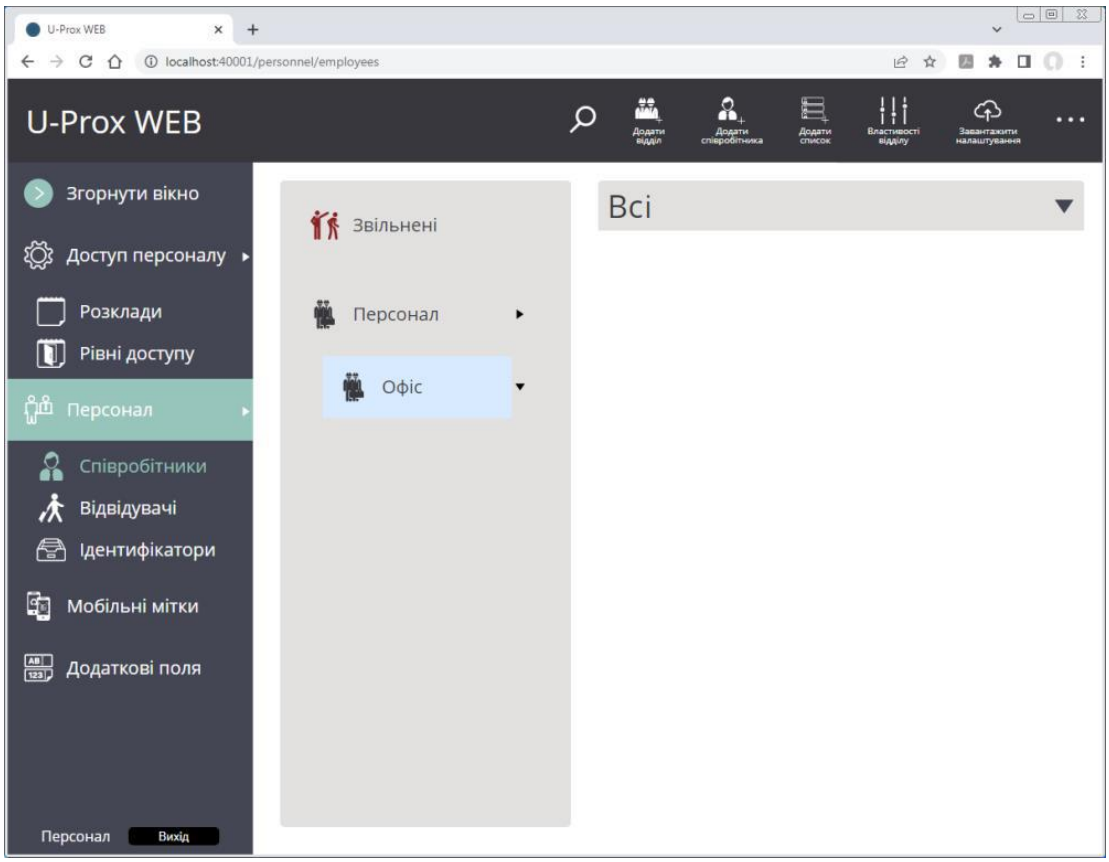
Всі користувачі повинні бути вписані у підрозділи, тому спочатку введемо деяку ієрархію відділів. Щоб додати відділ верхнього рівня, перейдіть до розділу "Співробітники" (ліворуч на панелі). Виберіть розділ "Персонал" та натисніть кнопку "Додати відділ".



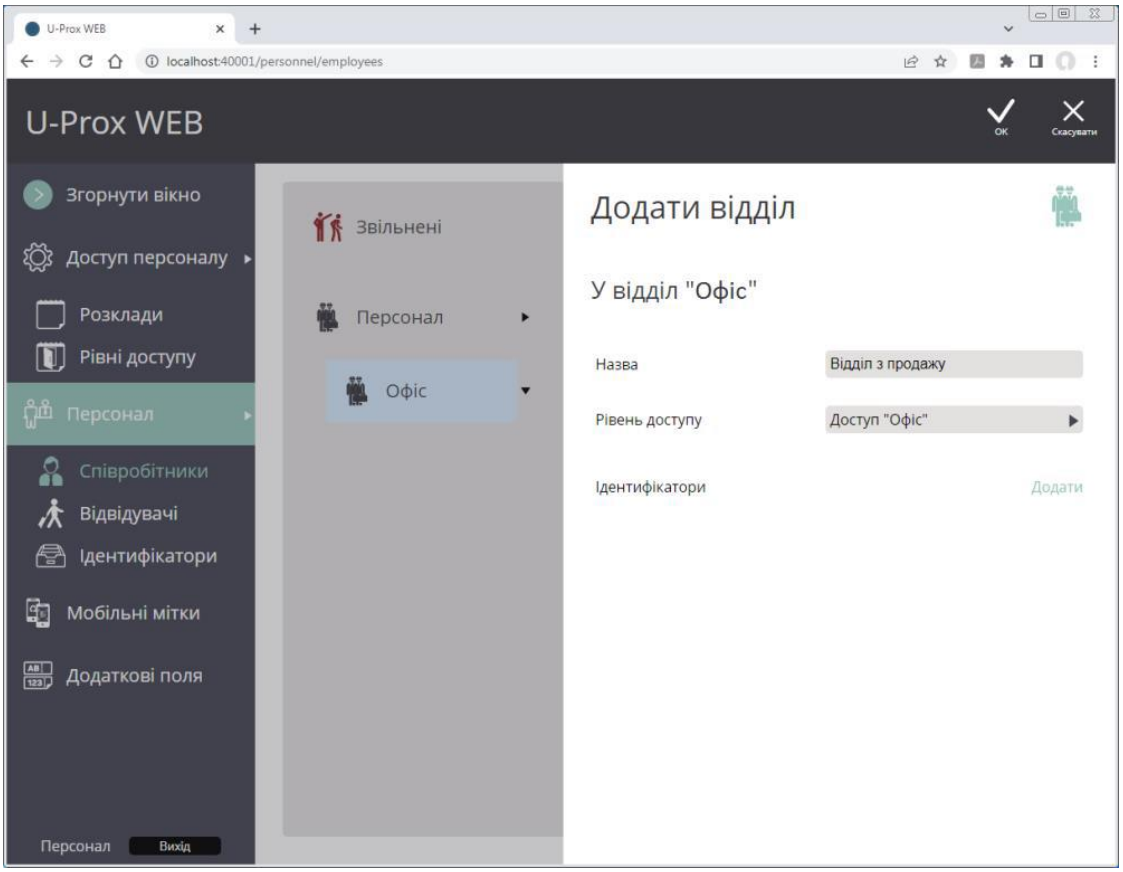
У вікні, що з'явиться, вкажіть назву відділу і рівень доступу, який можна буде використовувати для установки групового доступу.



Натисніть "OK", щоб зберегти зміни.

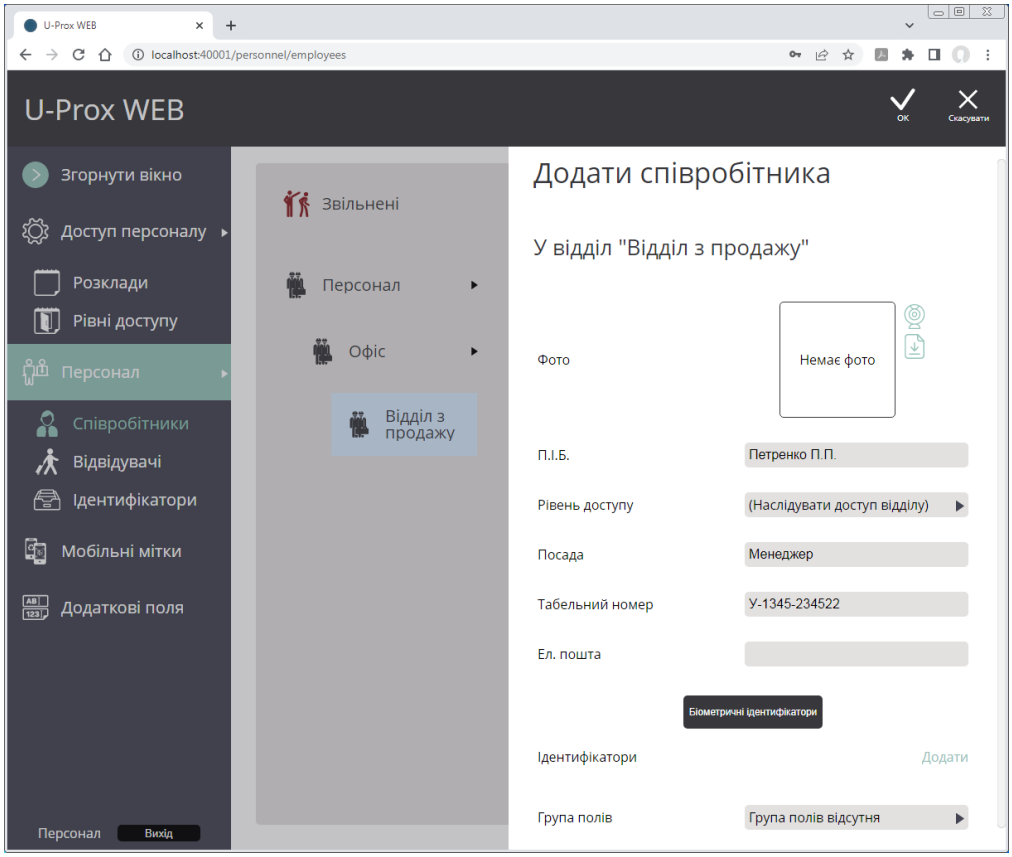


Для того, щоб додати підвідділ, виберіть існуючий відділ у дереві списків, та натисніть кнопку "Додати відділ".



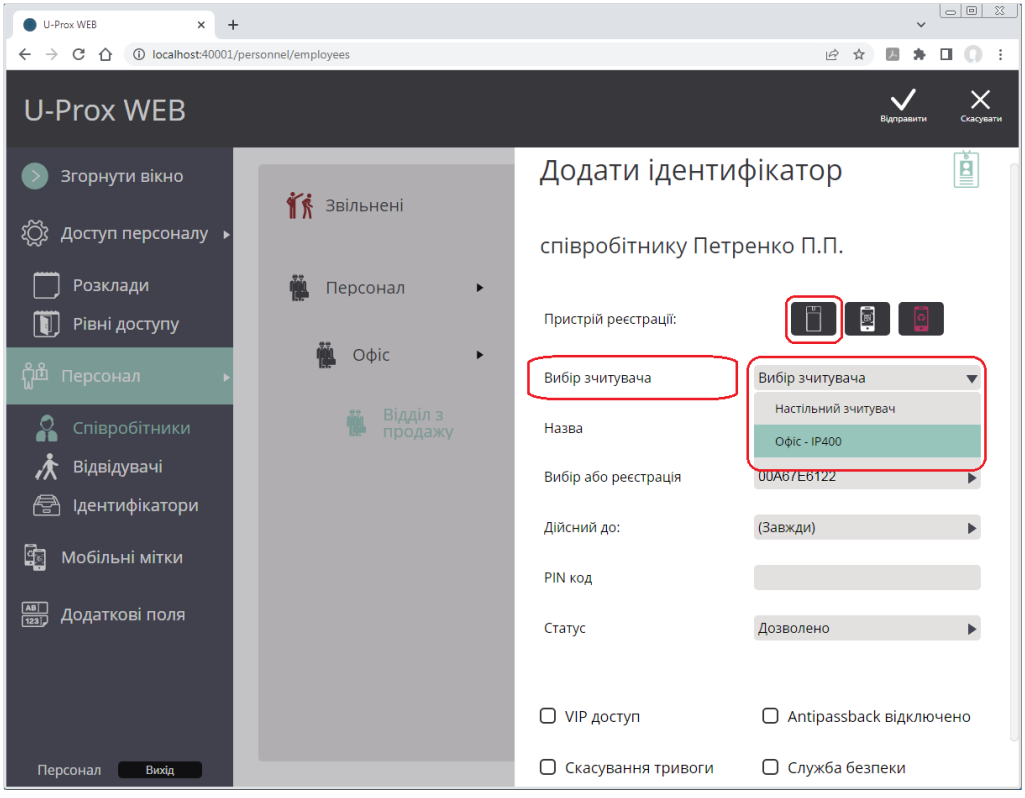
Додав ієрархію відділів, приступимо до додавання співробітників, які будуть проходити скрізь двері з певними ідентифікаторами. Щоб додати співробітника до відділу, виберіть

існуючий відділ у дереві списків та натисніть кнопку "Додати співробітника".



Щоб додати фотографію, клацніть на іконку "веб-камера" , для отримання фото з неї, чи на іконку "файл" , і в діалоговому вікні виберіть файл із фото співробітника.

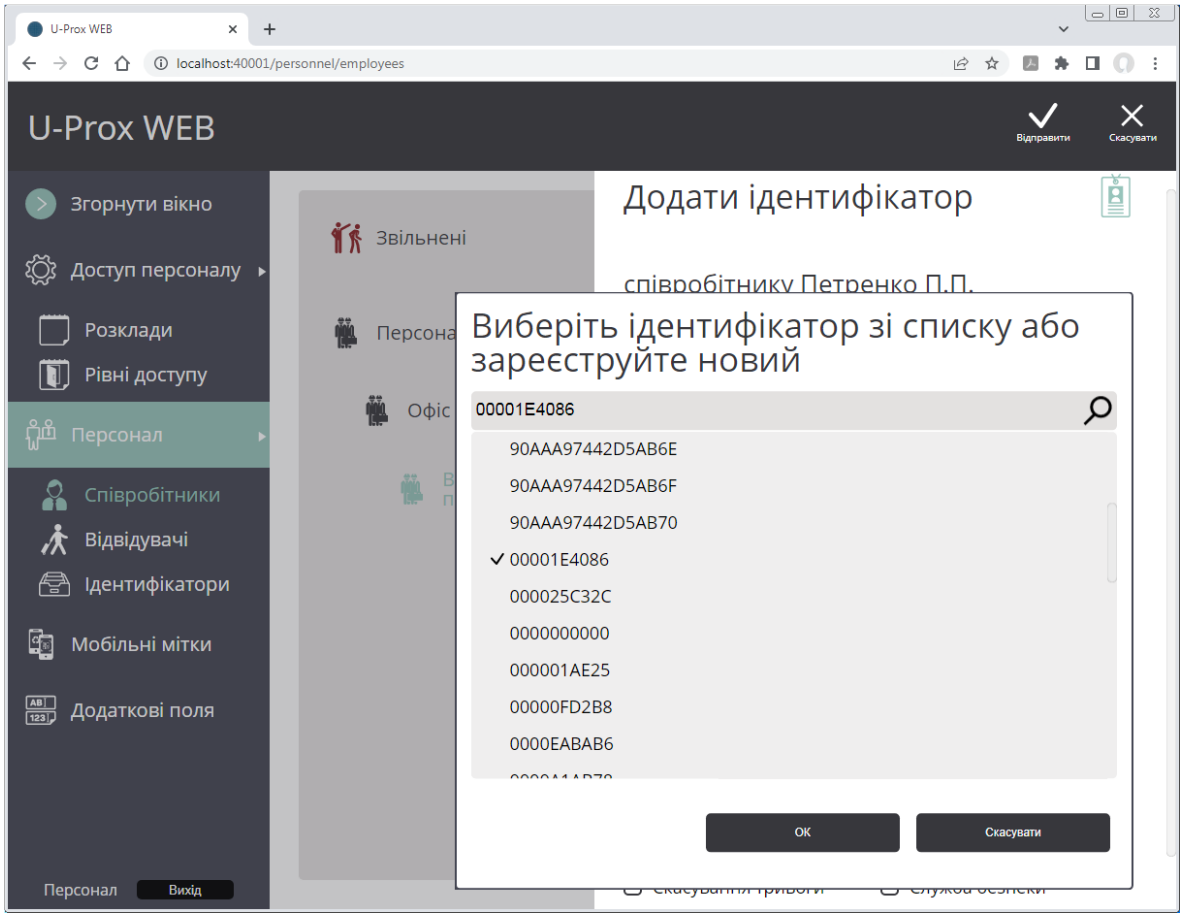
Далі слід додати ідентифікатор співробітнику. Для цього знизу натисніть посилання "Додати" навпроти "Ідентифікатори".



Надсилати мобільний ідентифікатор користувачу (якщо вони раніше внесені в базу даних пулу мобільних ідентифікаторів) на e-mail адресу користувача ми не станемо, тому що їх в нас немає, та зовсім опустим цей спосіб у цей статті. Також ми не станемо розглядати доступ через біометричні ідентифікатори типу обличчя і відбитків долонь та пальців, тому що ми не припасли їх, але як і зі звичайними зчитувачами U-Prox сумісен з біометричними терміналами ZKTeco. До того ж ми планували використовувати RFID карти.

Тому у вікні виберіть пристрій реєстрації ідентифікаторів.

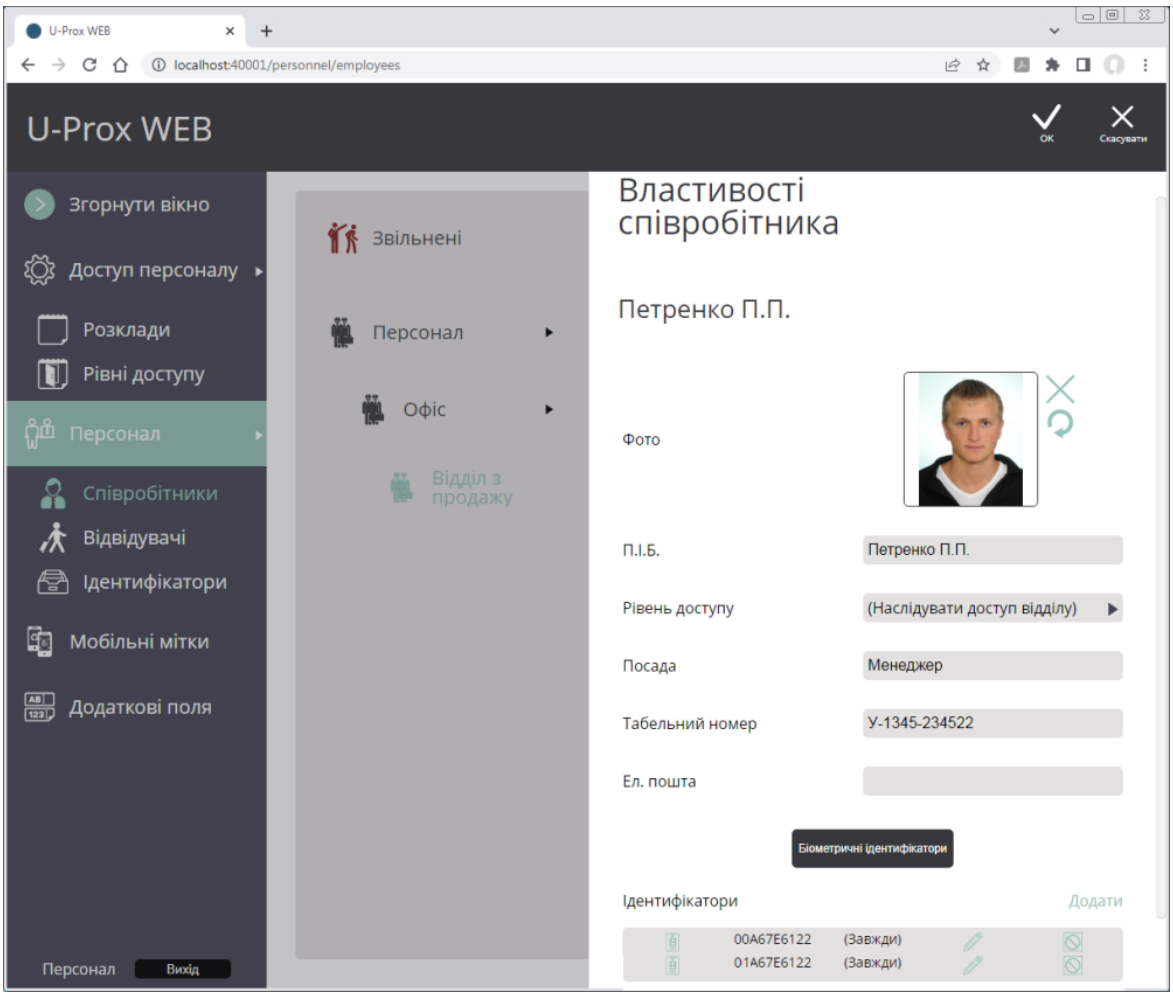
В нас у цьому експерименті немає настільного USB зчитувача "U-Prox Desktop", тому обираємо зчитувач із нашого контролера СКУД, що вже зареєстрований в системі



Ми можемо вибрати номер ідентифікатору зі зчитаних раніше чи зчитати прямо зараз. В нашому випадку простіше зчитати, але, якщо зчитувач далеко від комп'ютеру вигідніше зчитати номери заздалегідь.

Створення списку вільних ідентифікаторів ми розглянемо нижче, а поки невелике зауваження з безпосередньою реєстрацією.

Пам'ятайте, що у нас є 2 зчитувачі, один з яких ZKTeco? Так ось, нам через це доведеться завести картку 2 рази. Це тому, що зчитувач іншого виробника читає трохи інший код, тобто додає свої коригування.



По суті, це все, що потрібно було налаштувати для швидкого початкового запуску. В принципі нічого складного. Все, що зроблене - це елементарні пункти, які стосуються будь-якої системи доступу, але залишилася одна дрібниця, про яку інколи забувають.

Після програмування входів, виходів, прав доступу для власників ідентифікаторів, та інших параметрів, – необхідно завантажити контролер. Під час завантаження дані про налаштування потрапляють із бази даних до контролера.

Для цього лише треба натиснути кнопку «Завантажити налаштування», яка є на будь-якої сторінці змін конфігурацій.

Без необхідності не вимикайте пристрої один від одного, оскільки в цьому випадку може виникнути невідповідність між інформацією, що зберігається в них, і необхідність повторного завантаження. Операція завантаження проста, проте до з'ясування невідповідності, Ви можете отримувати ефекти, зовсім Вами не заплановані. Крім того, контролери можуть зберігати жорстко обмежену кількість подій, які комп'ютер постійно вичитує, зберігаючи у своїх базах даних. У разі тривалого відключення контролерів найстаріші події можуть бути безповоротно втрачені.

Далі можна приступати до перевірки роботи системи, але я обіцяв розповісти про введення невикористаних карток.

Для цього знов треба змінити оператора, натискаємо кнопку "Вихід", і, підтвердивши дію, заходимо в програму за даними ролі Бюро перепусток, переходячи до реєстрації ідентифікаторів.

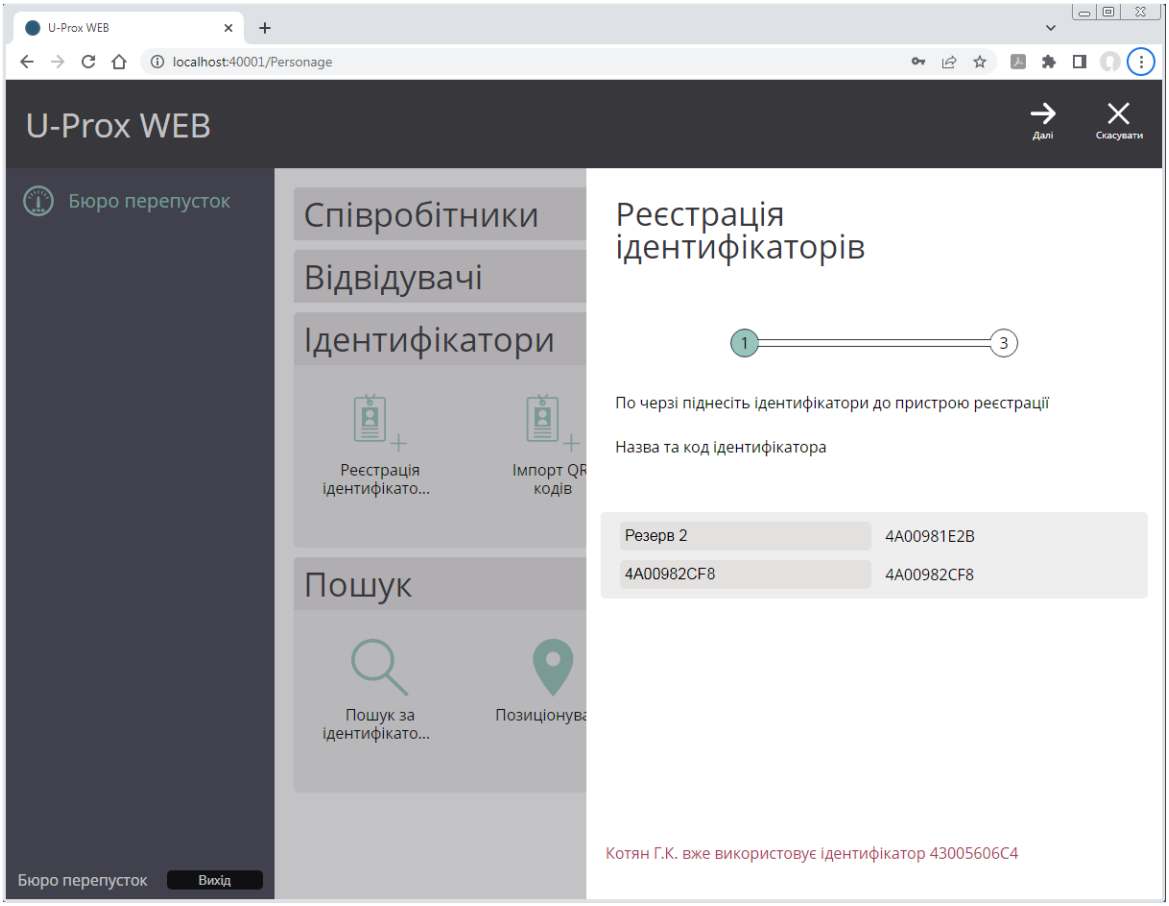
Цю операцію можна виконати відразу після додавання дверей, коли стануть активними зчитувачі, підключені до контролера.

Щоб додати ідентифікатори до системи, натисніть у розділі "Ідентифікатори" іконку "Реєстрація ідентифікаторів". Внесені ідентифікатори будуть знаходитися в списку невикористаних.

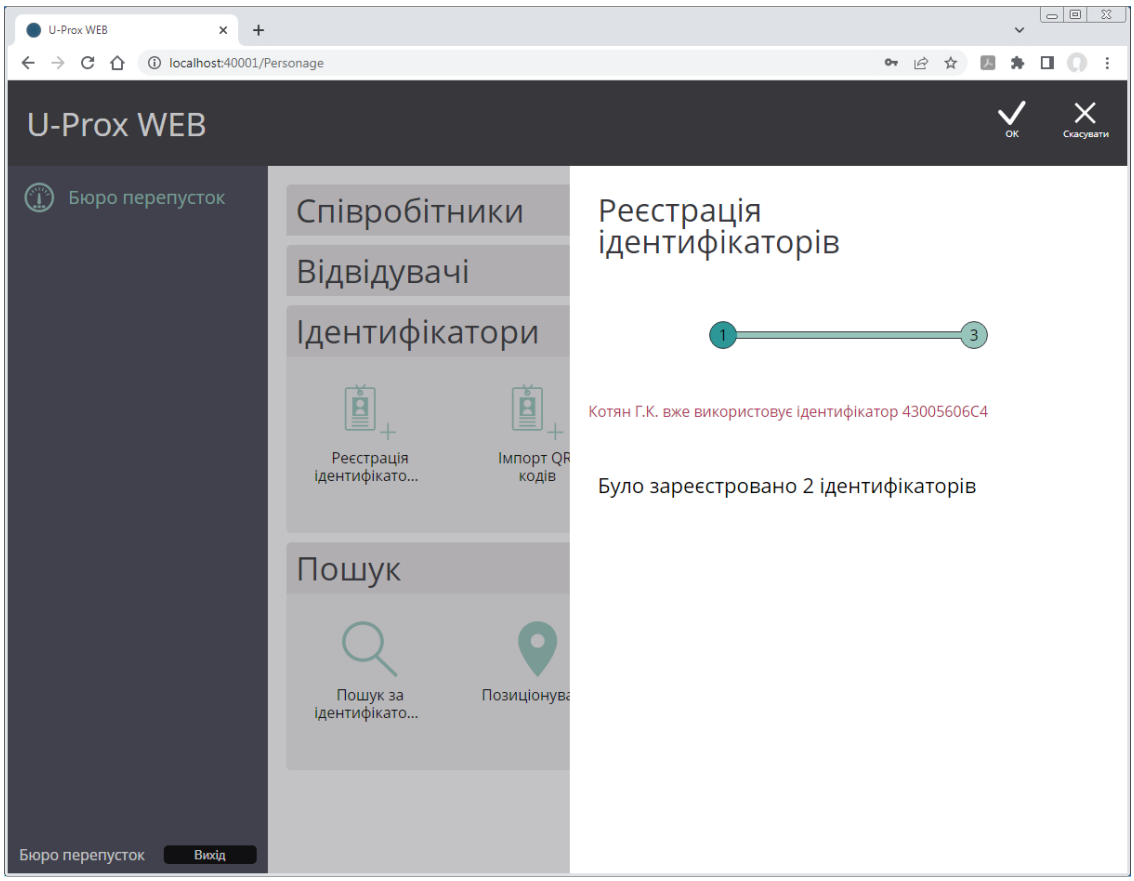
При піднесенні картки до зчитувача її код відображатиметься у вікні. Якщо картку вже було зареєстровано, цей факт буде позначено.

Так можна за раз внести в базу всі картки, підготовлені для передачі співробітникам, а також гостьові картки, що будуть видаватися тимчасово відвідувачам, якщо, звичайно, вони є і є час на прикладання.

Оператор може змінити назву зареєстрованої картки. Наприклад, відразу присвоїти карткам співробітників прізвища, а гостьовим - номери. До речі, якщо зчитувачі підтримують QR-коди, то їх можна ввести, як тимчасові ідентифікатори для відвідувачів.



Натисніть "Далі", і щоб зберегти зміни, натисніть "ОК".

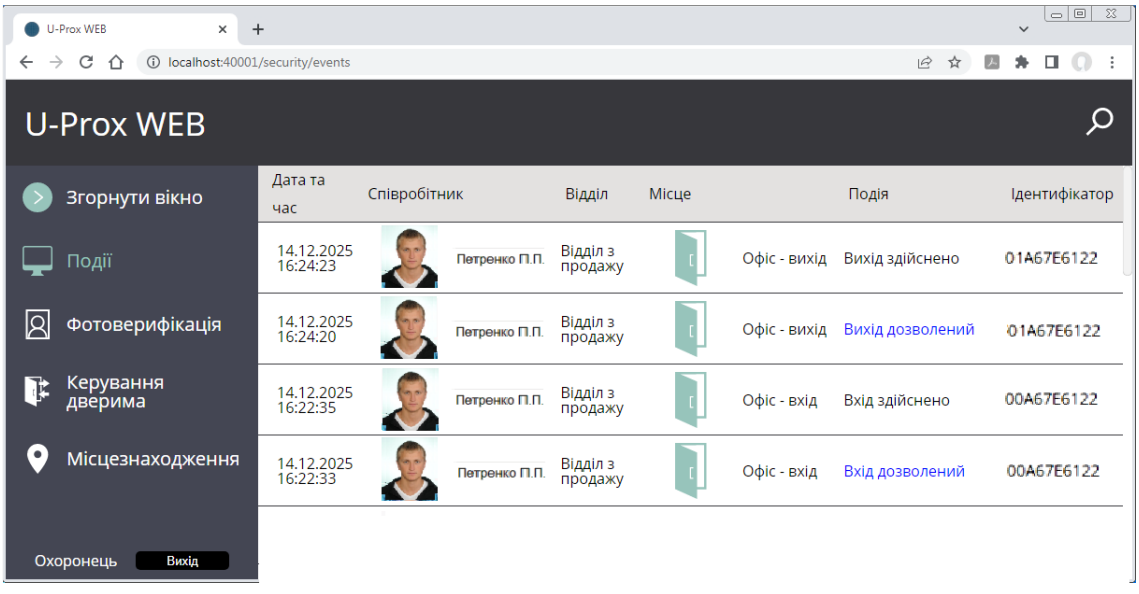


Але повернемося до швидкого запуску. Для перевірки налаштувань і правильності збірки знову міняємо оператора, натискаємо кнопку "Вихід", і, підтвердивши дію, заходимо в програму за даними охоронця, переходячи до моніторингу подій.

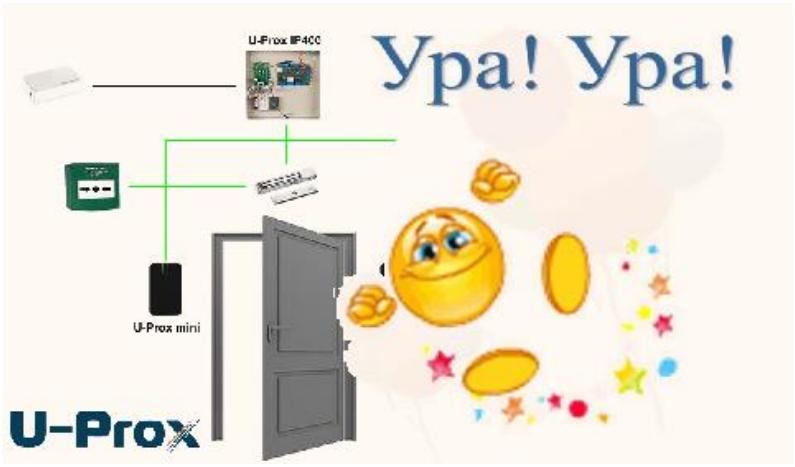
У процесі експлуатації системи відбуваються певні події: вхід і вихід співробітників, відкриття та закриття дверей, тощо. Всі ці події реєструються в журналах контролерів і далі, через комп'ютерну мережу, передаються на центральний сервер, і можуть бути відображені на користувацьких робочих місцях.

Перейдіть до розділу "Події" (ліворуч на панелі). Буде відображено поточний журнал подій.

Усе, ми можемо перевіряти прохід.



Перевіряємо роботу. Підносимо картку до першого зчитувача - все ок, вхід пройшов успішно, до другого – ок, як бачимо все працює у нас відбувся вхід та вихід.

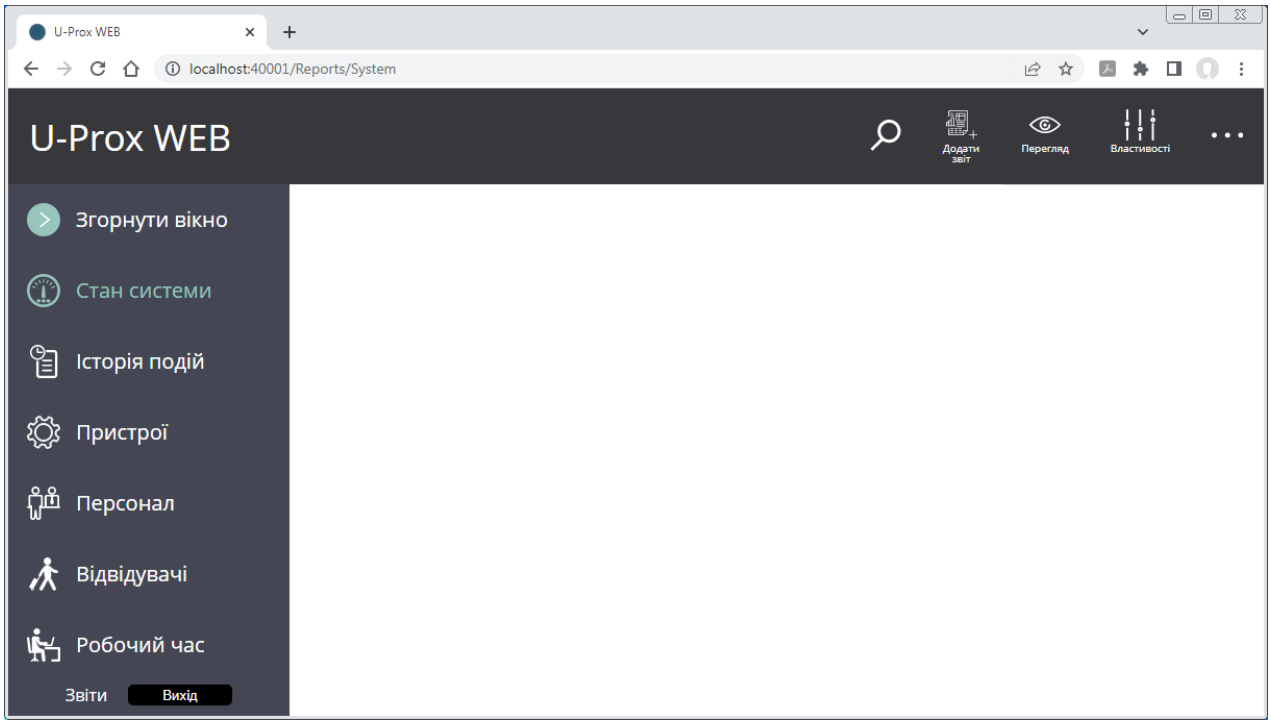


СИСТЕМА НАСТРОЄНА!

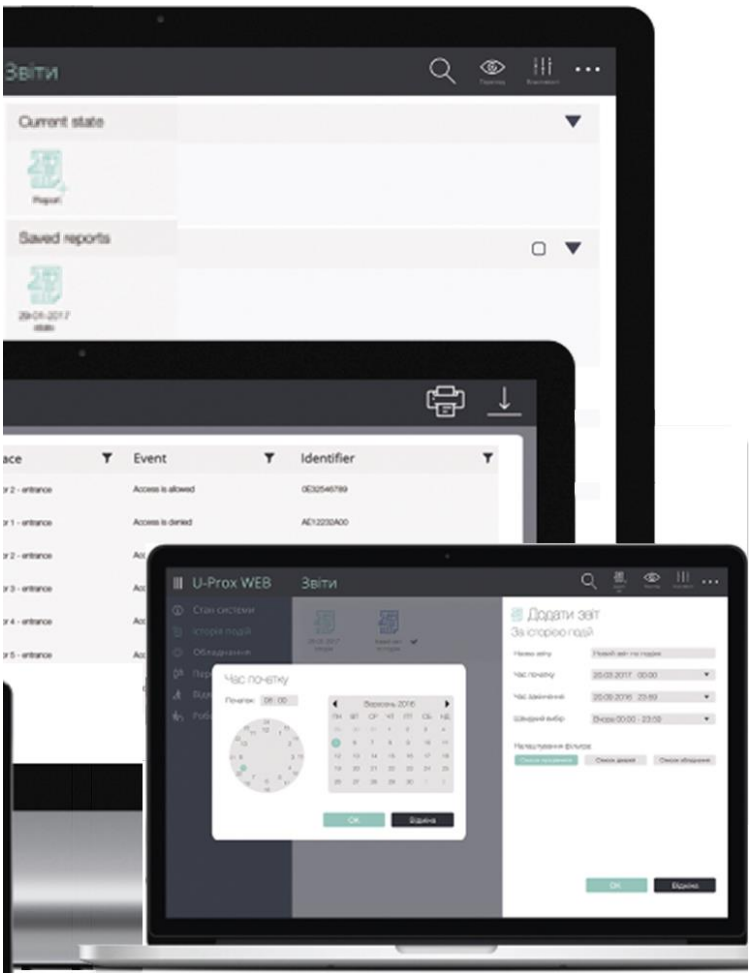
Натискаємо кнопку" Вихід", і, підтвердивши дію, виходимо з акаунту охоронця.

Це мабуть все, але для повноти картини тепер давайте розглянемо звіти. До речі, щодо звітів, мало хто зустрічав інші програми курування СКД, які мають настільки гнучкі звіти.

Робоче місце «Звіти» дозволяє формувати звіти за станом системи, подій, персоналу і відвідувачів, вести облік робочого часу.

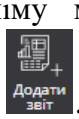


Для звітів в принципі не обов'язково заводити окремого оператора, а можна додати видимість цього інтерфейсу будь-якому іншому оператору, в залежності від структури організації.



Як видно в системі передбачені 6 шаблонів звітів, а не готові кнопки для видачі результату. На їх основі можна сформувати нескінченну різноманітність звітів, вносячи коригування і підключаючи видимість даних. Свої звіти можна зберігати в системі, щоб, використовуючи вже їх, як шаблони, отримувати саме ті дані, які потрібні для організації.

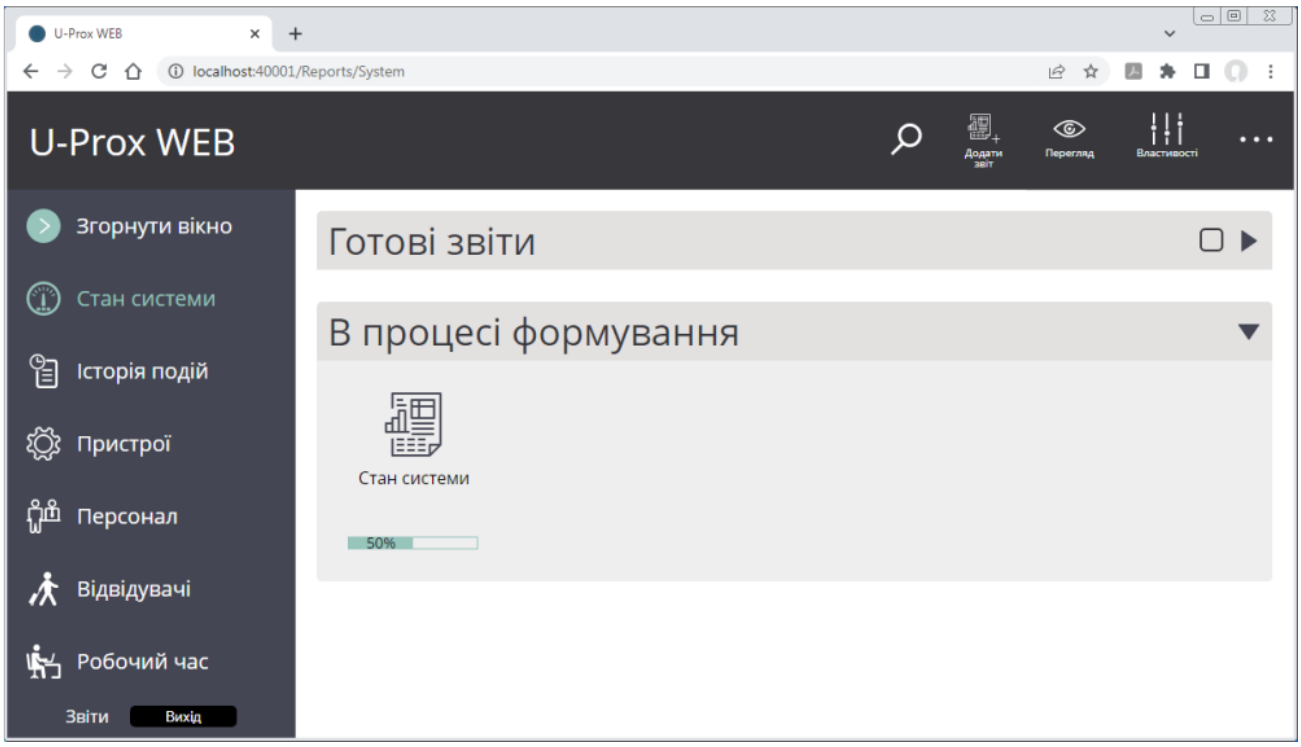
Звіт "Стан системи" призначений для отримання зведеної інформації про стан усіх пристроїв та дверей у системі.

Перейдіть до розділу "Стан системи" та у верхньому меню натисніть "Додати звіт" 

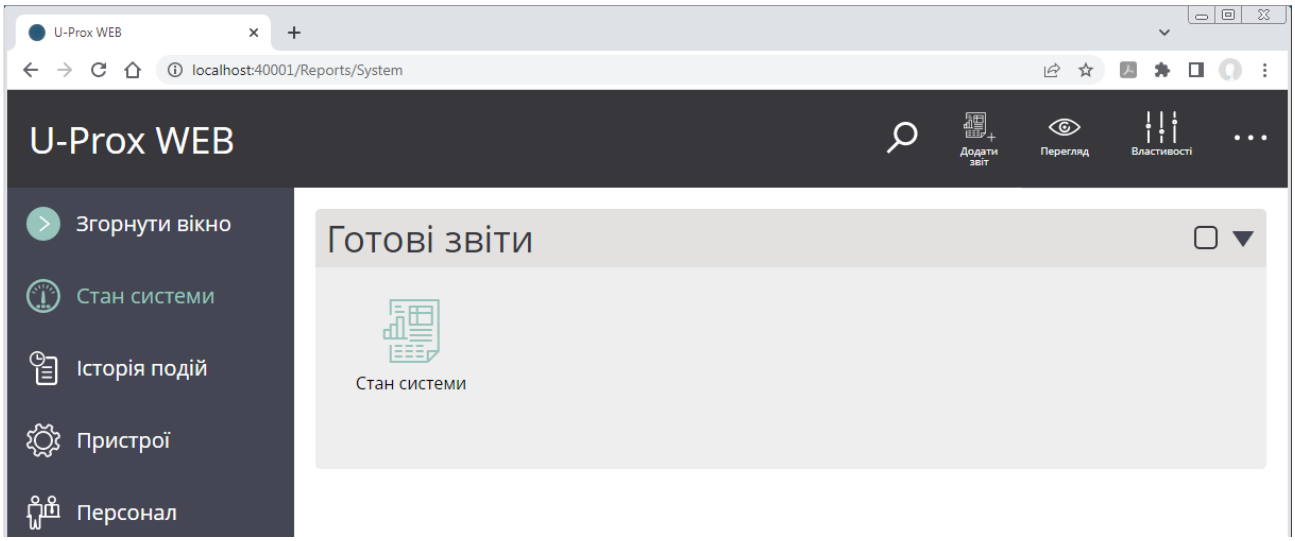
.

У вікні, що відкрилося введіть назву звіту та натисніть "ОК".

Буде розпочато формування звіту, що відображається в категорії "В процесі формування":

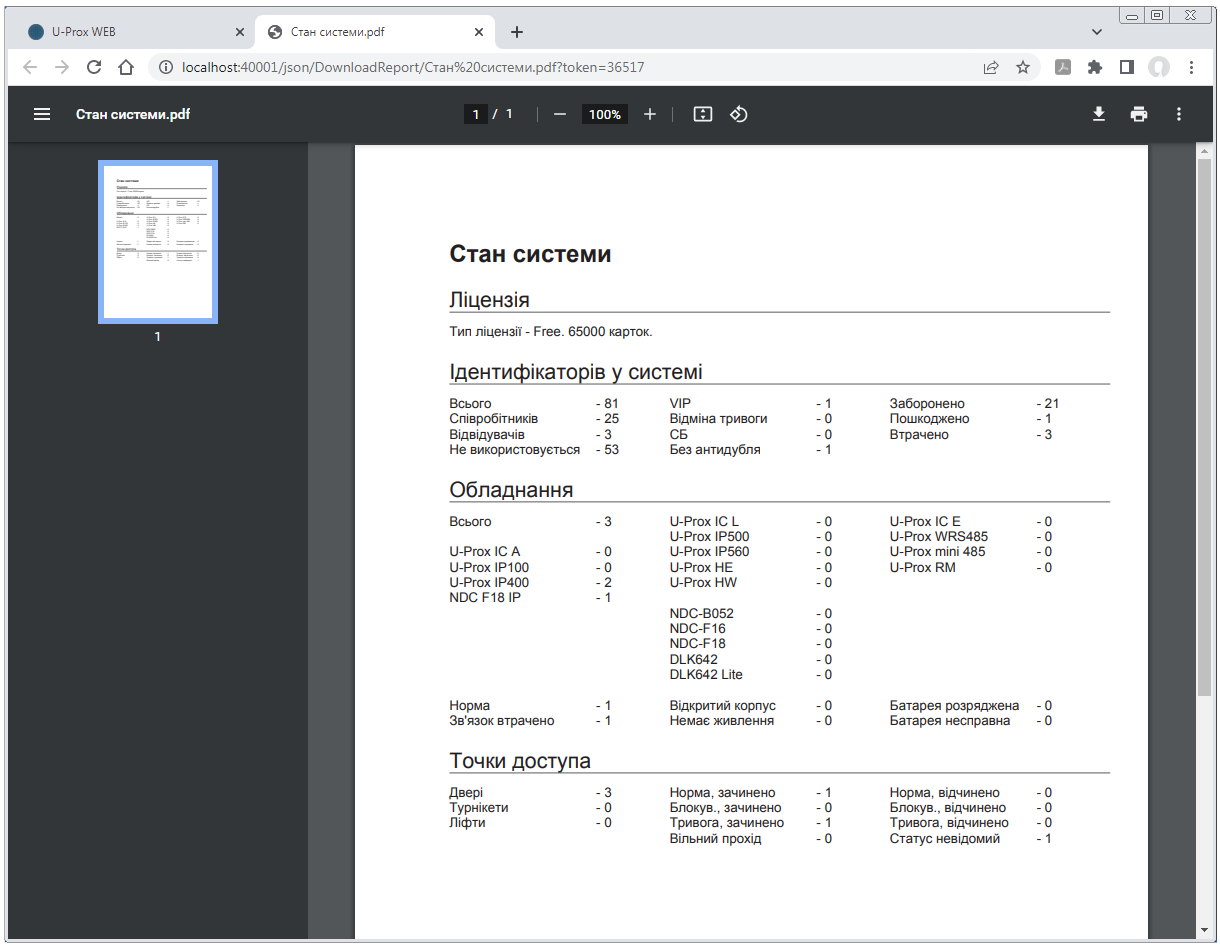


Як буде сформовано, звіт перейде до категорії "Готові звіти":

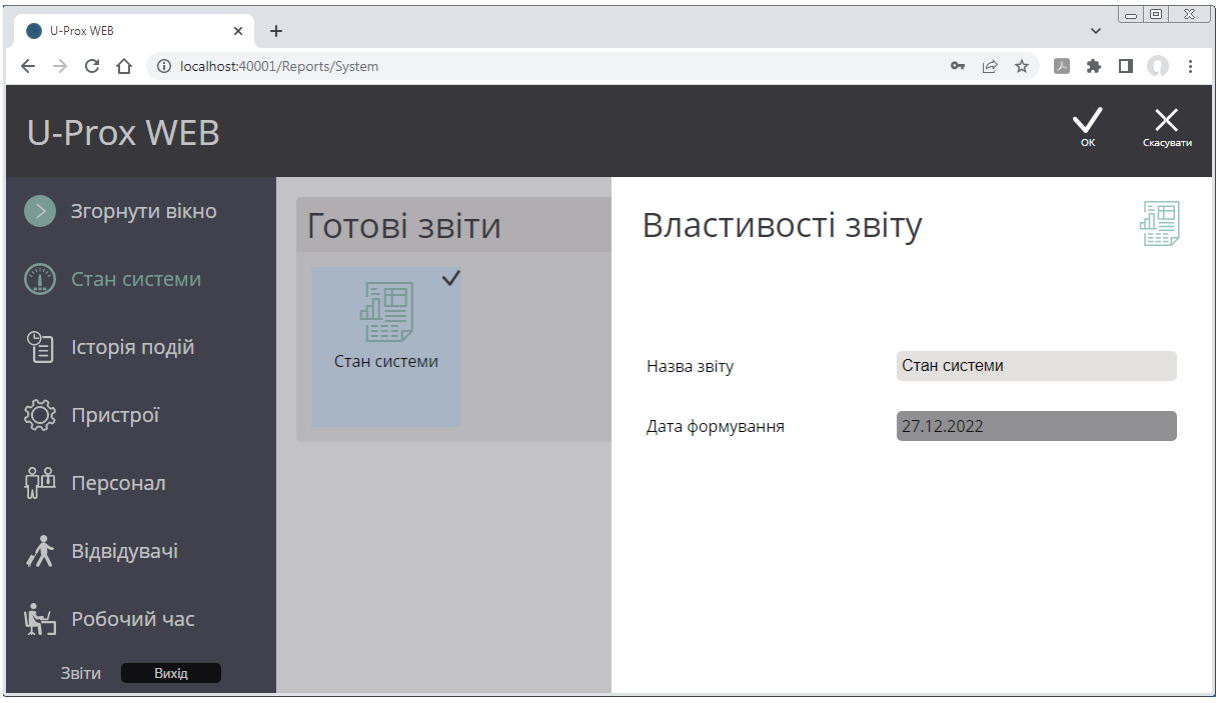


Щоб переглянути звіт, відмітьте його ☑, та натисніть у меню "Перегляд" 

:



Щоб змінити назву звіту чи внести зміни параметрів, якщо це можливо, відмітьте його ☑, та натисніть зверху в меню "Властивості":



Звіт "Історія подій" є простою вибіркою з журналу подій. В процесі формування звіту необхідно вказати дату і час початку, дату і час кінця інтервалу, до якого повинні входити події, співробітники, та пристрої, дії яких спричинили подію, а також необхідні типи подій.

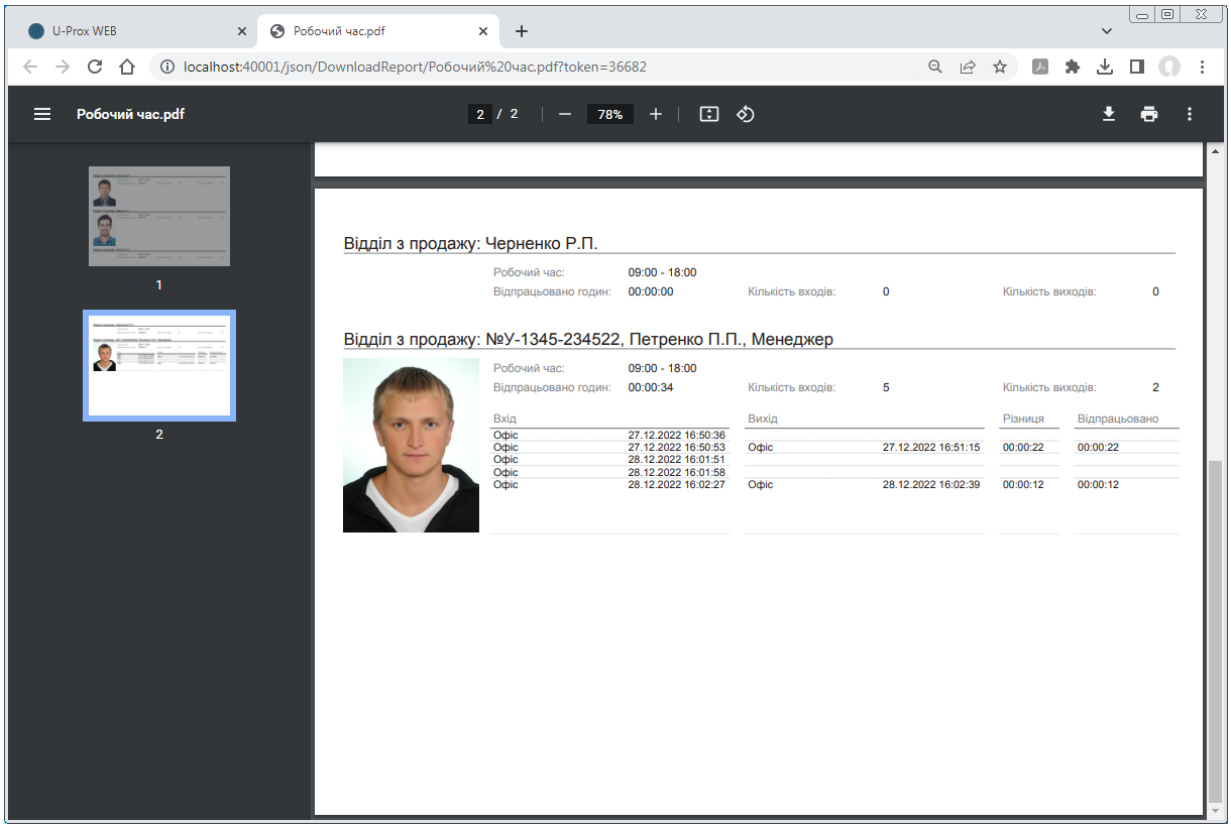
Звіт "Пристрої" призначений для отримання зведеної інформації щодо конфігурації всіх пристроїв (шлейфи, виходи) та точок доступу в системі.

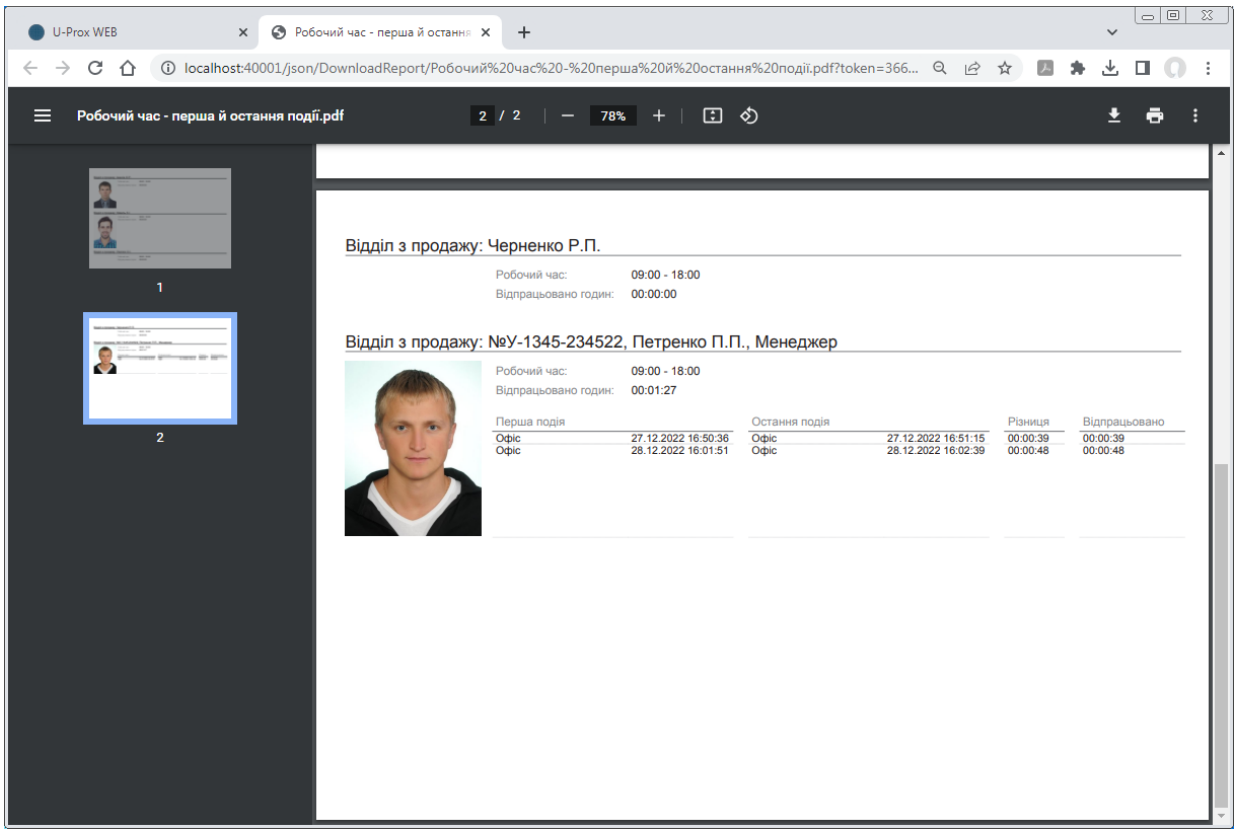
Звіт "Персонал" призначений для отримання зведеної інформації щодо співробітників, з їхніми правилами доступу та ідентифікаторами.

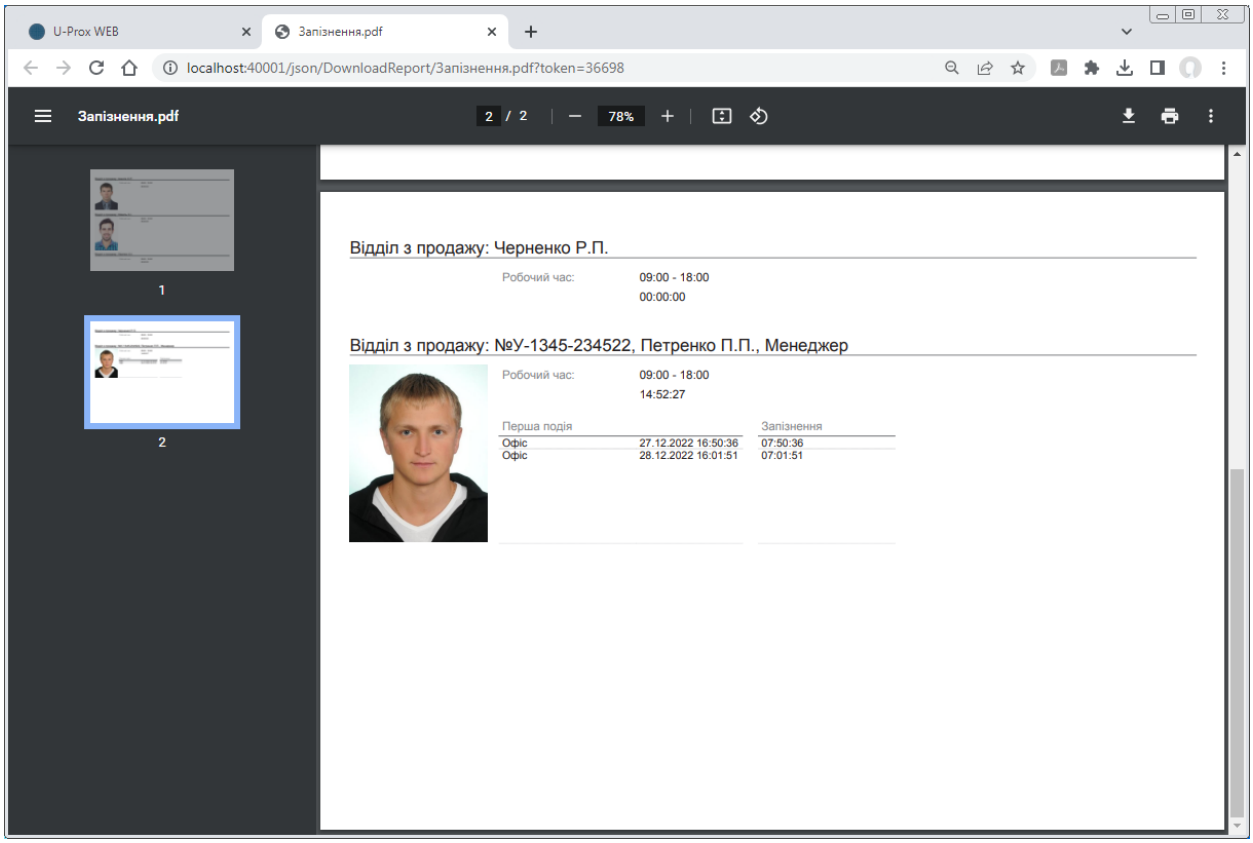
Звіт "Відвідувачі" призначений для отримання зведеної інформації щодо відвідувачів, з їхніми правилами доступу та ідентифікаторами.

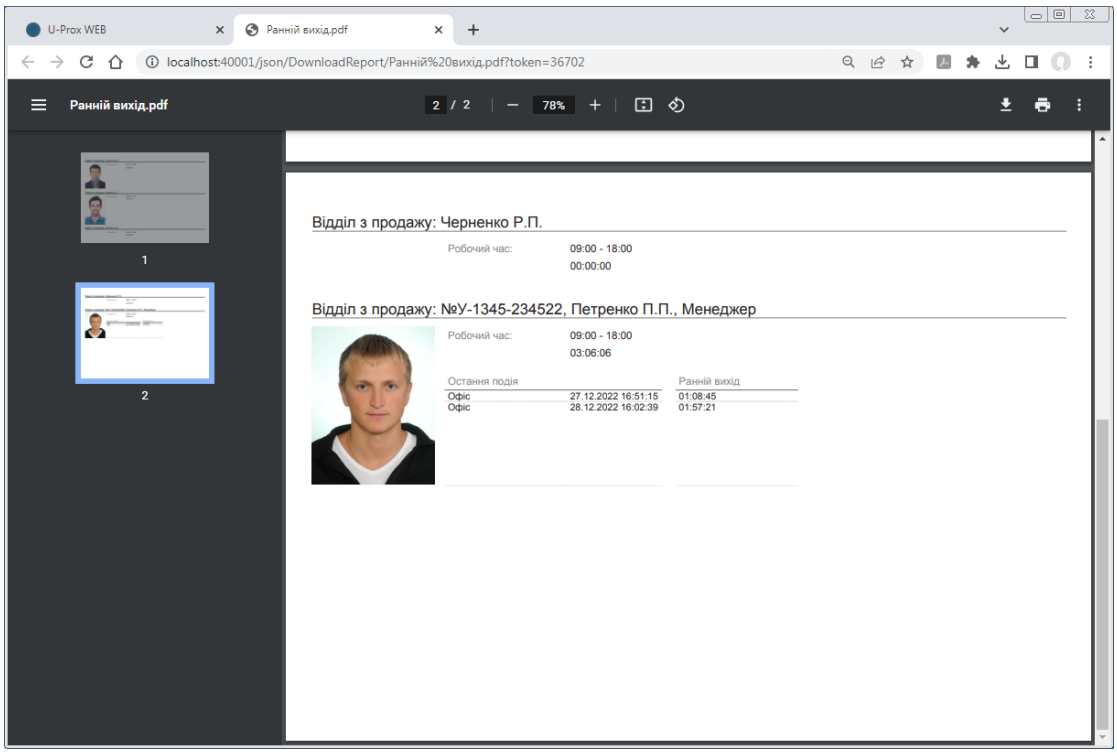
Звіт "Робочий час" використовується для простого розрахунку робочого часу за вказаним у звіті робочими годинами. Залежно від налаштувань дозволяє сформувати місячний табель відпрацьованого часу, або простий звіт по персоналу для обліку відпрацьованого часу, фактів нез'яви, затримки, та запізнення.

Змінюючи параметри цього звіту, окрім звичайного табелю та інших стандартних звітів можливо отримати ось таки окремі звіти, наприклад:



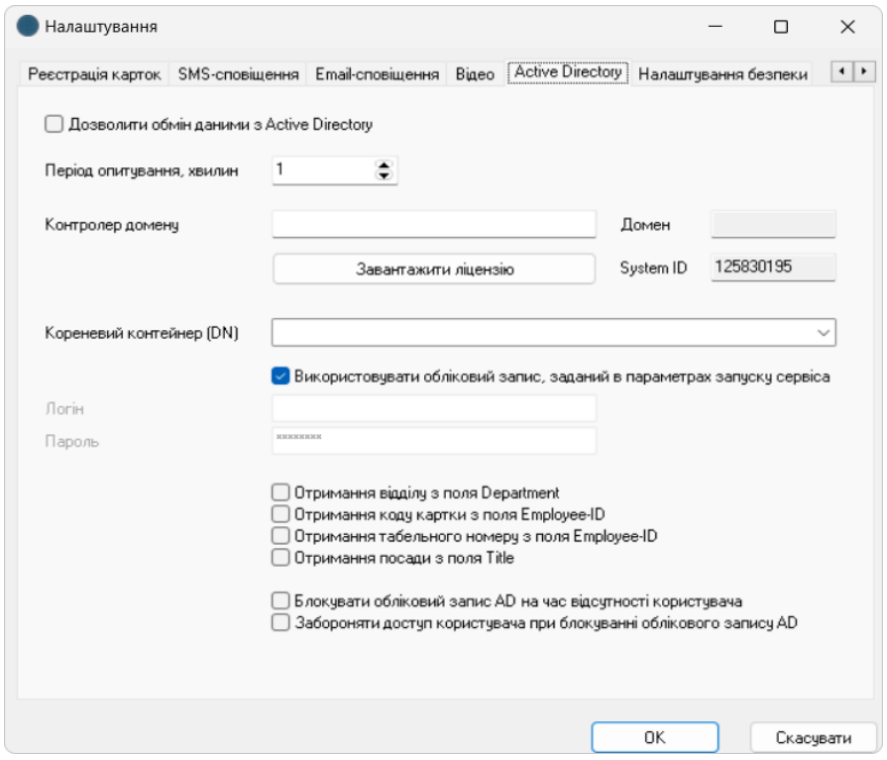

U-Prox WEB
Робочий час - перша й останн
localhost:40001/json/DownloadReport/Робочий%20час%20-%20перша%20й%20остання%20події.pdf?token=366...
Робочий час - перша й остання події.pdf
2 / 2
78%
1
2
Відділ з продажу: Черненко Р.П.
Робочий час: 09:00 - 18:00
Відпрацьовано годин: 00:00:00
Відділ з продажу: №У-1345-234522, Петренко П.П., Менеджер
Робочий час: 09:00 - 18:00
Відпрацьовано годин: 00:01:27
Перша подія
Остання подія
Різниця
Відпрацьовано
Офіс 27.12.2022 16:50:36 Офіс 27.12.2022 16:51:15 00:00:39 00:00:39
Офіс 28.12.2022 16:01:51 Офіс 28.12.2022 16:02:39 00:00:48 00:00:48


U-Prox WEB
Запізнення.pdf
localhost:40001/json/DownloadReport/Запізнення.pdf?token=36698
Запізнення.pdf
2 / 2
78%
1
2
Відділ з продажу: Черненко Р.П.
Робочий час: 09:00 - 18:00
00:00:00
Відділ з продажу: №У-1345-234522, Петренко П.П., Менеджер
Робочий час: 09:00 - 18:00
14:52:27
Перша подія
Запізнення
Офіс 27.12.2022 16:50:36 07:50:36
Офіс 28.12.2022 16:01:51 07:01:51



Як висновок поглянемо на побудовану нами систему ще раз. Ось так швидко і просто можна додати обладнання та налаштувати права доступу співробітнику. Як ви помітили ніяких труднощів це не викликає.

Тепер згадаємо про деякі функціональні можливості, що ми не втілили в цьому проекте: фотобейджі, тимчасові плани, антидубль, інтеграція відео подій, інтеграція біометрії, гнучкі звіти, а ще з використанням спеціального ПЗ “Модуль роботи з LDAP сервісами та Active Directory” U-Prox Web може інтегруватися з Active Directory та використовувати профілі користувачів, прізвища, заповнювати поля, активувати чи деактивувати дозвіл на прохід з корпоративного серверу тощо.



Ще одним плюсом цієї системи є підтримка API, тобто ви можете розробити власні модулі та використовувати їх в особистих цілях наскільки вам зручно чи зручно для підприємства.

Ще один плюс це "гаряча" заміна контролерів. Якщо якийсь із контролерів з якоїсь причини вийшов з ладу у великій мережі, вам не потрібно заново прописувати двері, заново прописувати розклади в ньому і так далі. Просто змінюєте контролер та завантажуєте дані. Все більше нічого не треба робити, тільки попереднє налаштування мережі.

І це далеко не весь перелік всього того що вміє U-Prox.

Ось така СКД українського виробництва U-Prox Access Control.