

Призначена для автоматизації процесів
в медичних закладах

**Інструкція користувача модулем
Система безпеки.
Двофакторна автентифікація.**

Зміст

1. Загальні правила безпеки.....	3
2. Перший вхід. Створення паролю в МІС.....	4
3. Повсякденний вхід в програму	7
4. Принцип роботи "Один користувач — один сеанс"	9
5. Захист від підбору паролів	10

1. Загальні правила безпеки

ЕСОЗ запроваджує нові правила безпеки при роботі в МІС.

Ці правила розповсюджуються на всіх користувачів МІС незалежно від рівнів доступу та спеціалізацій.

1. Подвійний захист входу (2FA)

Відтепер для входу в систему недостатньо лише пароля - запроваджується **двофакторна автентифікація**.

- **Як це працює:** Окрім звичайного пароля (те, що ви знаєте), потрібно буде підтвердити вхід іншим способом (те, що є тільки у вас — наприклад, код на електронну пошту). Це гарантує, що навіть якщо зловмисник дізнається ваш пароль, він не зможе зайти у ваш кабінет.

2. "Один користувач — один сеанс"

Для запобігання ситуаціям, коли під одним логіном працюють кілька людей одночасно:

- Система дозволить лише **одну активну сесію**.
- Якщо ви зайдете в МІС на іншому комп'ютері або в іншому браузері, робота на попередньому пристрої автоматично завершиться. Це критично для захисту персональних даних пацієнтів.

3. Захист від підбору паролів

Система стане суворішою до помилок при вході:

- Якщо пароль введено неправильно **5 разів поспіль**, обліковий запис буде автоматично заблоковано на **5 хвилин**.
- Це зроблено для того, щоб роботи (програми-зломщики) не могли підібрати ваш пароль шляхом перебору варіантів.

4. Контроль доступу та конфіденційність (Захист від IDOR)

Було оновлено внутрішні алгоритми перевірки прав. Тепер система перевіряє право доступу до кожного окремого документа чи картки пацієнта щоразу, коли ви їх відкриваєте.

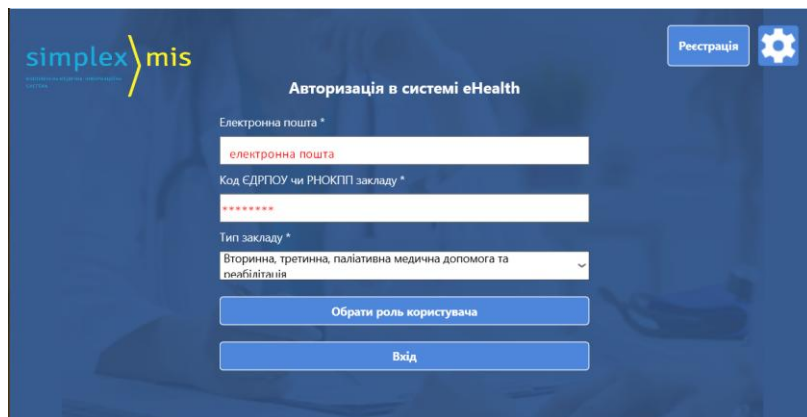
- Навіть якщо хтось спробує вручну змінити номер документа в посиланні (URL), система не дозволить переглянути дані, на які у користувача немає офіційного дозволу.

5. Шифрування та технічна безпека

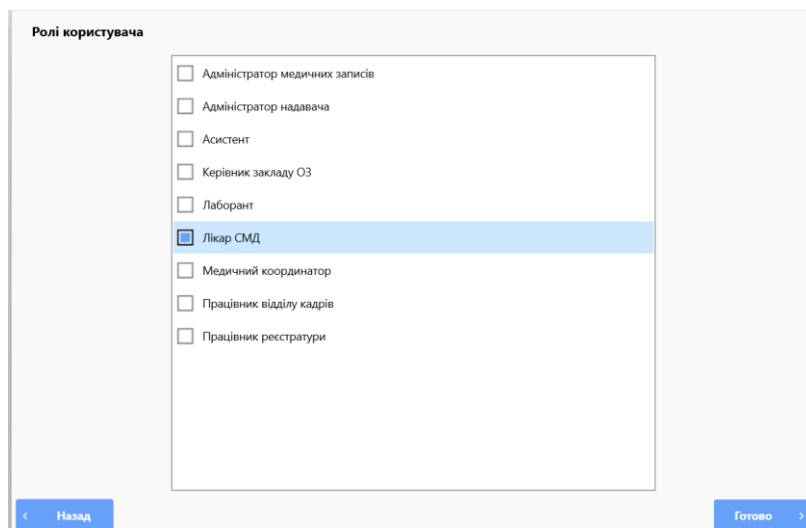
- **Безпечне з'єднання:** Уся комунікація між вашим комп'ютером і сервером тепер відбувається виключно через сучасні зашифровані канали (протокол TLS 1.2+).
- **Приховані ключі:** Технічні ідентифікатори системи (наприклад, `client_secret`) тепер повністю ізольовані від кінцевого користувача, що виключає можливість стороннього втручання в роботу програми.

2. Перший вхід. Створення паролю в МІС.

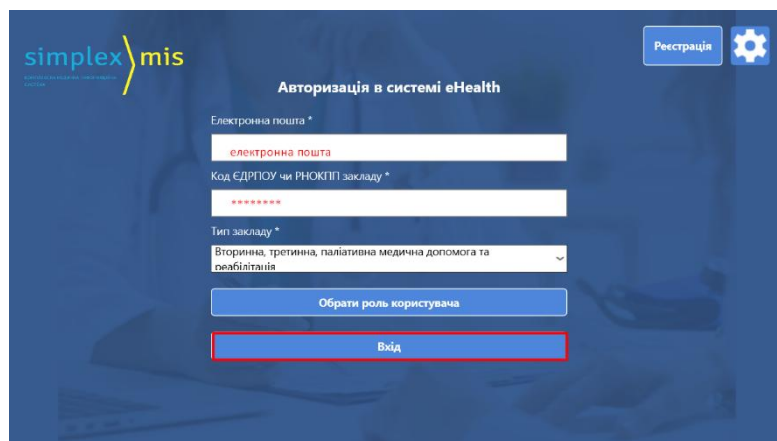
1. Запускаємо програму з ярлика на робочому столі
Заповнюємо поля:
 - електронна пошта користувача;
 - код ЄДРПОУ чи РНОКПП закладу;
 - тип закладу (обираємо з переліку).



2. Натискаємо кнопку **Обрати роль користувача**.
Обираємо роль в залежності від рівня доступу.
Натискаємо **ГОТОВО**.



3. Натискаємо кнопку **Вхід**.



4. Відкривається інформаційне вікно.
Натискаємо **Продовжити**.

Увага: Необхідна реєстрація облікового запису МІС

Відповідно до вимог наказу Національної служби здоров'я України від 04.11.2025 № 826 щодо безпеки та функціональності медичних інформаційних систем, для продовження роботи вам необхідно створити персональний обліковий запис.

Для реєстрації виконайте наступні кроки:

1. Пройдіть авторизацію в системі eHealth (на наступному кроці).
2. Встановіть індивідуальний пароль для безпосереднього доступу до МІС.

Важливо: Задля захисту медичних даних подальший вхід у систему здійснюватиметься з використанням двофакторної автентифікації (2FA).

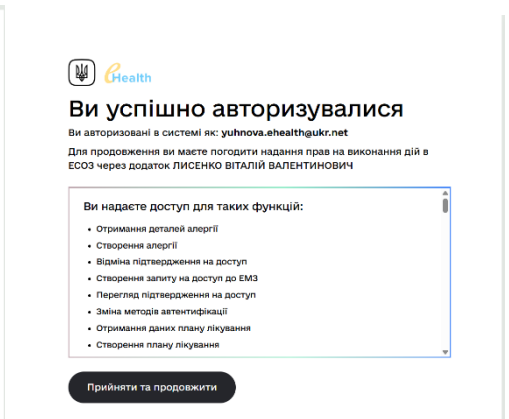
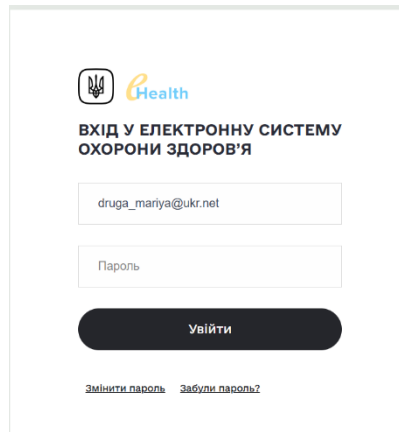
[Продовжити](#) [Скасувати](#)

5. Авторизація в ЕСОЗ:

Користувач вводить свій пароль eХелс.

Натиснути кнопку **Увійти**.

Кнопка **Прийняти та Продовжити**.

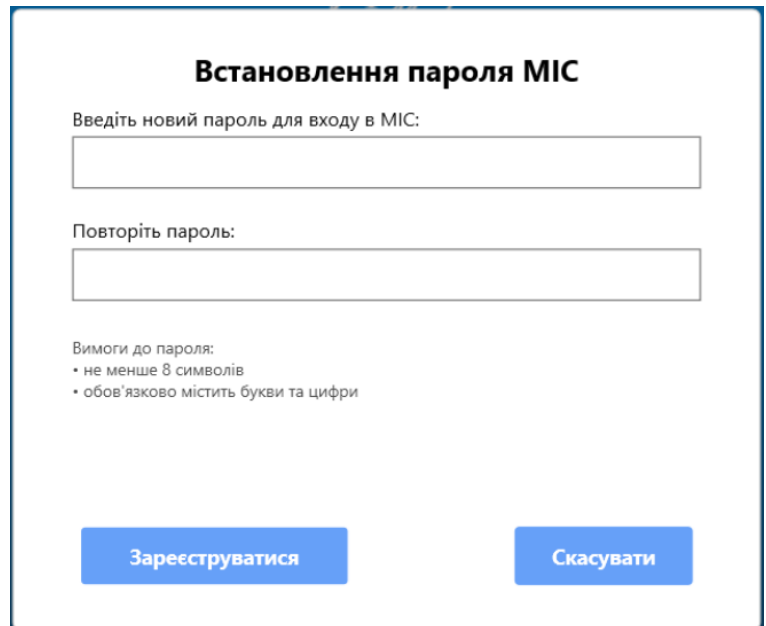


6. Відкривається вікно "Встановлення пароля в МІС".

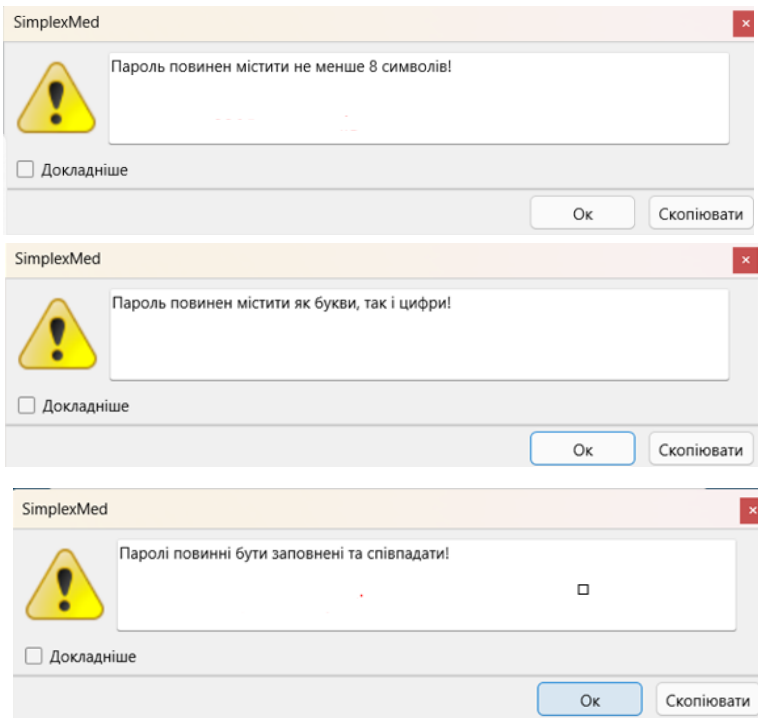
- Треба ввести новий пароль для входу в МІС;
- повторити пароль;
- Натиснути кнопку **Зареєструватися**.

7. Для створення пароля діють певні правила, а саме:

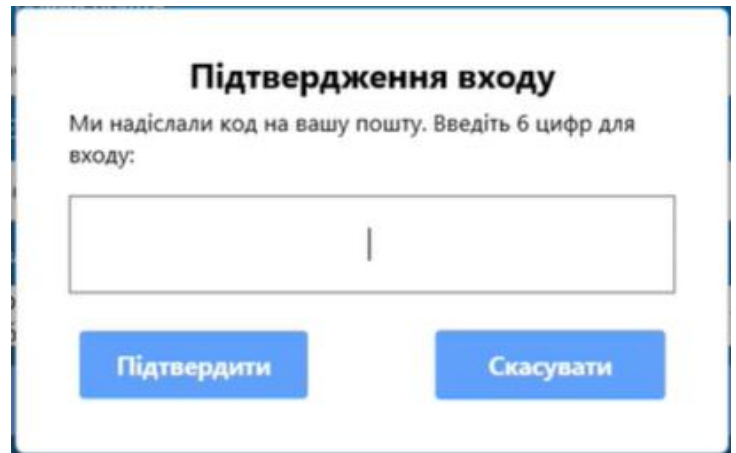
- пароль має містити не менше 8 символів;
- пароль має містити літери та цифри.



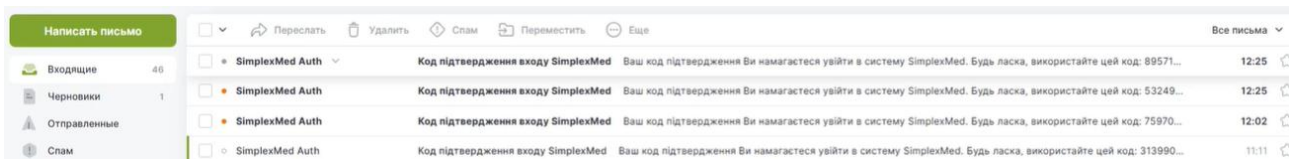
8. Якщо користувач не виконає правила створення пароля, то система покаже повідомлення



9. Після успішної реєстрації пароля в МІС відкривається вікно.



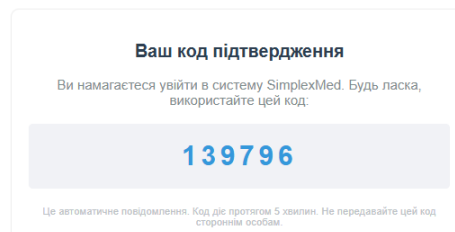
10. Треба перейти в свою поштову скриньку, яка використовується вами для авторизації в ЕСОЗ. Знайти на пошті повідомлення від МІС.



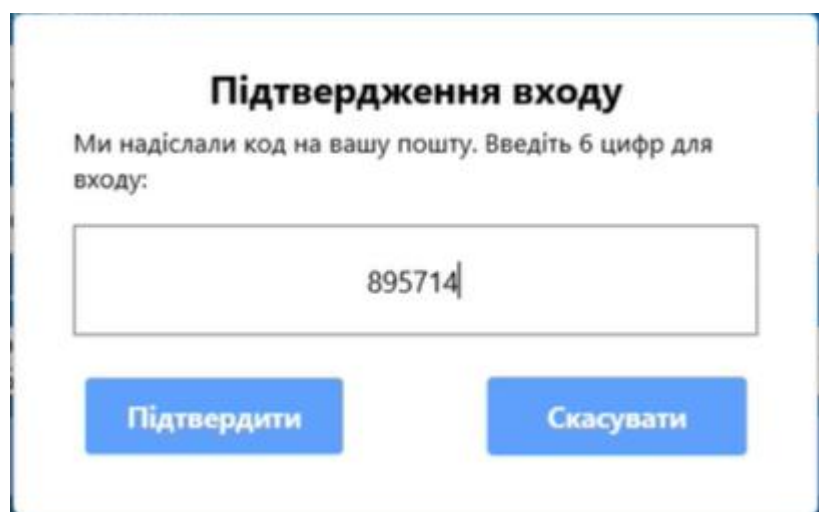
11. Відкрити повідомлення та скопіювати код підтвердження. Код містить 6 цифр.

Код підтвердження входу SimplexMed

SA SimplexMed Auth <no-reply@simplex-med.com>
Кому: yuhnova.ehealth@ukr.net



12. Вставити код у відповідну клітину. Натиснути **Підтвердити**.

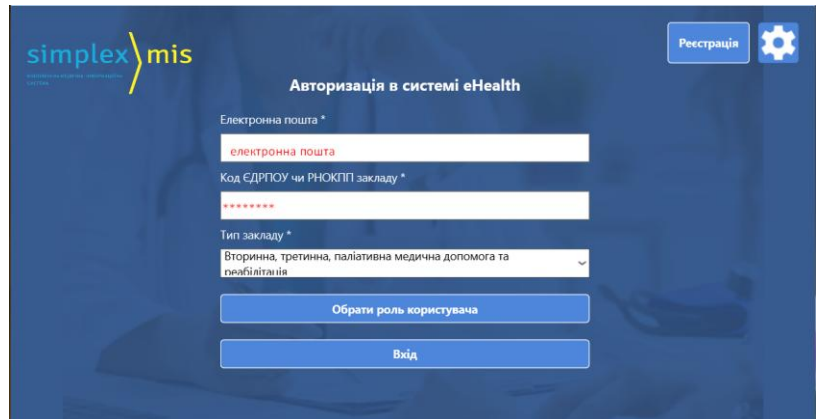


13. Після цього первинний (після впровадження заходів безпеки) вхід у МІС буде виконаний. Програма готова для використання.

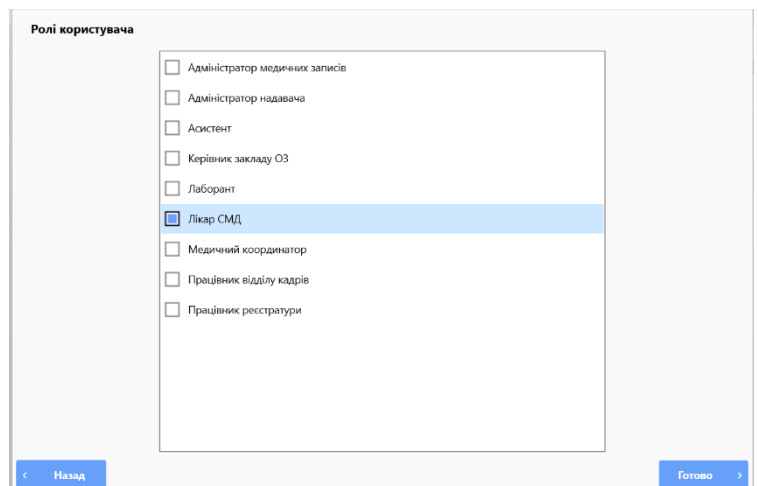
3. Повсякденний вхід в програму

Для захисту медичних даних подальший вхід у систему здійснюватиметься з використанням двофакторної автентифікації (2FA).

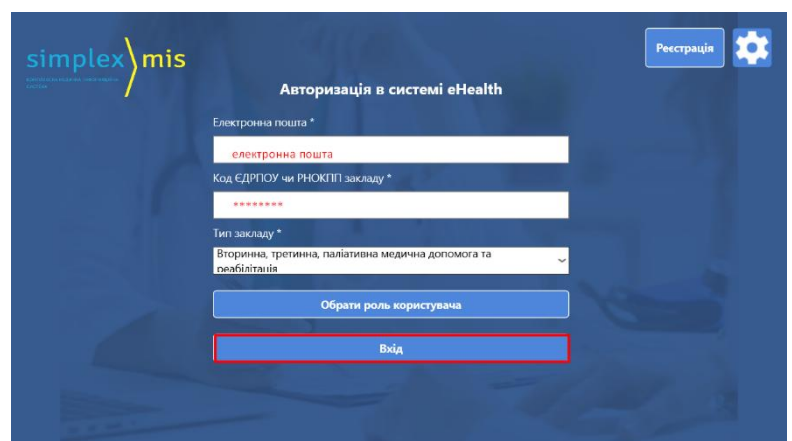
1. Запускаємо програму з ярлика на робочому столі
Заповнюємо поля:
 - електронна пошта користувача;
 - код ЄДРПОУ чи РНОКПП закладу;
 - тип закладу (обираємо з переліку).



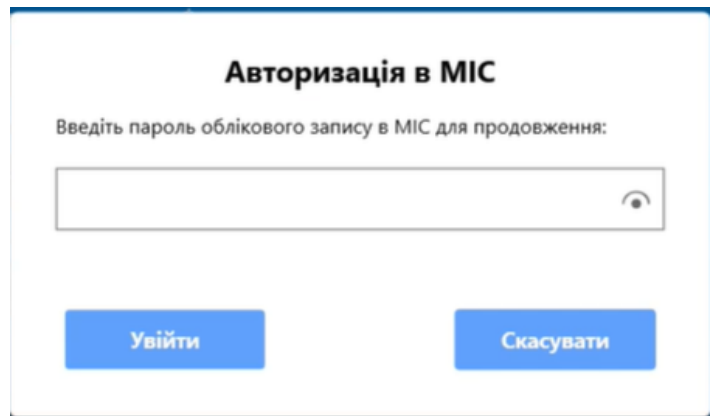
2. Натискаємо кнопку **Обрати роль користувача**.
Обираємо роль в залежності від рівня доступу.
Натискаємо **ГОТОВО**.



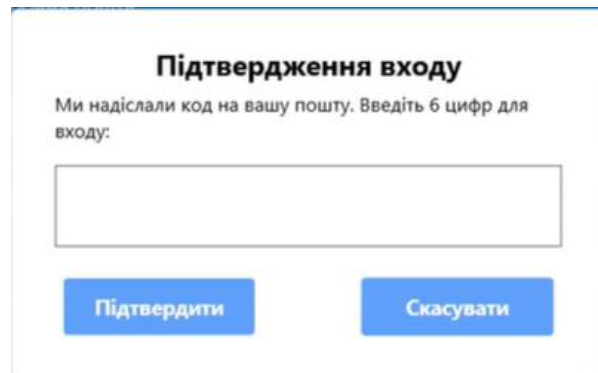
3. Натискаємо кнопку **Вхід**.



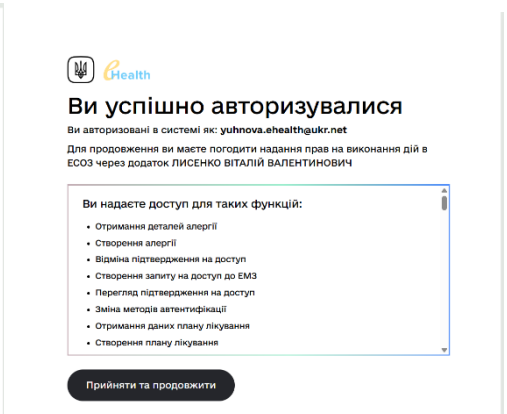
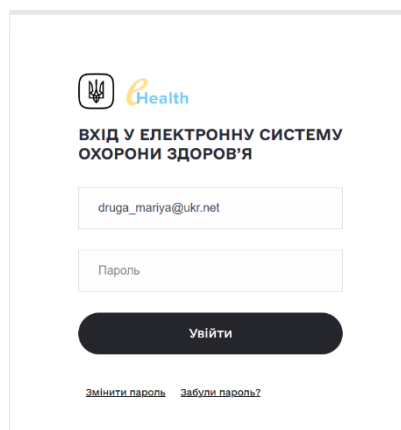
4. Відкривається вікно «Авторизація в МІС»
5. Вводимо раніше створений при першому вході пароль облікового запису. Натискаємо кнопку **Увійти**.



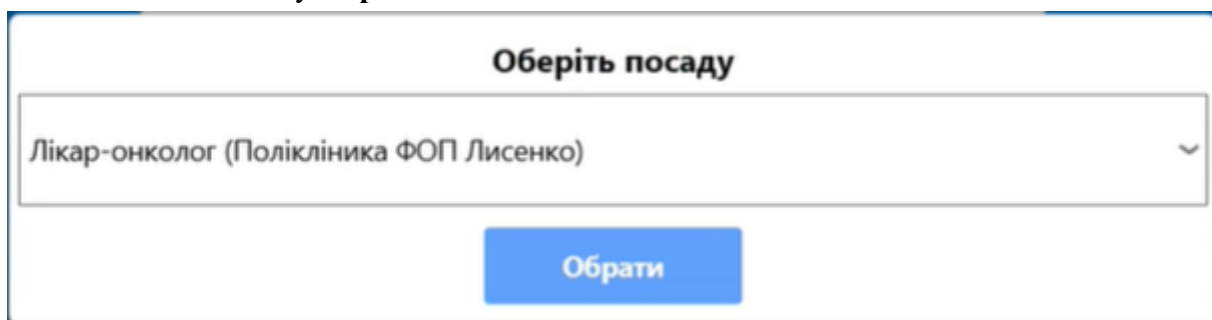
6. На електронну пошту прийшов код підтвердження.
7. Вносимо код.
8. Натискаємо кнопку **Підтвердити**.



9. Відкривається вікно для авторизації в ЕСОЗ.
10. Користувач вводить свій пароль eХелс. Натиснути кнопку **Увійти**. Кнопка **Прийняти та Продовжити**.



11. Відкривається вікно «Оберіть посаду».
- Необхідно обрати посаду, за якою користувач буде вносити записи в ЕСОЗ. Натискаємо кнопку **Обрати**.



12. Після цього вхід у МІС буде виконаний. Програма готова для використання.

4. Принцип роботи "Один користувач — один сеанс"

Після впровадження заходів безпеки кожний користувач має працювати тільки в одному робочому вікні.

Система дозволить лише **одну активну сесію**

Якщо на іншому комп'ютері / ноутбучі буде виконано повторний вхід, перший сеанс автоматично закриється.

При виконанні будь-якого запиту в новій сесії, у старій сесії користувач отримає інформаційне повідомлення про помилку та ця сесія буде завершена.

5. Захист від підбору паролів

1. Якщо користувач ввів пароль для МІС неправильно **5 разів поспіль**, обліковий запис буде автоматично заблоковано на **5 хвилин**.
2. Система рахує неправильні введення паролю та повідомляє користувача про невдалу спробу повідомленням.

Авторизація

Невірний пароль.

OK

3. Після п'ятої невдалої спроби система виводить повідомлення на екран та блокує користувача на 5 хвилин.

Безпека

Тимчасове обмеження доступу.

Ви ввели неправильний пароль 5 разів поспіль. Доступ до системи обмежено на 5 хвилин для запобігання несанкціонованому входу.

OK

4. Навіть, якщо користувач згадає правильний пароль до МІС, система не дозволить ввести пароль раніше ніж мине строк тимчасового обмеження доступу.
Користувач отримає повідомлення:

Безпека

Обліковий запис заблоковано

OK