📑 Оновлення безпекових вимог до МІС: чому це важливо

В умовах постійних кібератак з боку ворога на державні реєстри та системи, захист медичних даних стає пріоритетом національного рівня.

Саме тому посилення безпеки МІС та ЕСОЗ — це частина загальнонаціональної стратегії кіберзахисту.

Останні випадки кібератак як на український приватний сектор, так і на державну цифрову інфраструктуру, наочно продемонстрували: подібні атаки можуть повністю паралізувати роботу всієї сфери, заблокувавши доступ до важливих даних та сервісів.

При цьому переважна більшість кіберзлочинів починається саме з компрометації облікових записів користувачів (викрадення логінів та паролів).

Чому посилено вимоги з безпеки для МІС?
В оновлені технічні вимоги до МІС були включені розширені безпекові вимоги. Хоча базові вимоги до кібербезпеки існували й раніше, зараз вони стали чіткішими та більш деталізованими.

Чим зумовлена необхідність змін:

1. **Протидія кіберагресії ворога:** в Україні триває стійка тенденція до посилення безпекових заходів у всіх державних системах. Тому посилення вимог до взаємодії з ЕСОЗ – це частина загальнонаціональної стратегії цифрового захисту України від кібертероризму.

2. **Глобальне зростання кількості кібератак:** на практиці фіксується сплеск атак, спрямованих на викрадення облікових даних медичних працівників, у тому числі, через фішинг.

3. **Міжнародні стандарти:** вимоги адаптовані до сучасних світових практик інформаційної безпеки, зокрема рекомендацій **NIST** (Національний інститут стандартів і технологій США) та **OWASP** (Open Web Application Security Project).

Які безпекові вимоги увійшли до технічних вимог:

- **Обов'язкова двофакторна автентифікація (2FA).**

Для входу в МІС ористувач повинен підтвердити особу додатковим фактором.

Крім логіну та пароля, другим фактором автентифікації, як правило, є одноразовий код, який генерується у відповідному застосунку (Google Authenticator, Microsoft

Authenticator), надсилається у SMS/месенджер, або ж використання апаратного ключа (токена) чи біометричних даних (відбиток пальця, розпізнавання обличчя) тощо.

> **Навіщо:** це суттєво знижує ймовірність компроментації облікового запису, навіть якщо ваш пароль було викрадено.

- **Обмеження мультисесійності: принцип «Один користувач – один пристрій»**

Впроваджується контроль активних сесій. Якщо ви заходите в систему на новому пристрої, ваш попередній сеанс на іншому комп'ютері автоматично завершується.

> **Навіщо:** це унеможливлює паралельне використання вашого облікового запису сторонніми особами та допомагає миттєво виявити підозрілу активність.

Нагадуємо:

Як і раніше усі медичні працівники мають працювати через власний обліковий запис в МІС, підтверджувати дії власним електронним підписом, адже, як і лікарі, молодші медпрацівники несуть відповідальність за них.

- **Уточнено правила захисту від перебору паролю (Brute-force)**

Встановлено обмеження: у разі 5-разового неправильного введення пароля доступ до системи для цього користувача блокується на 5 хвилин.

- **Захист від несанкціонованого перегляду (IDOR)**

МІС тепер перевірятиме права доступу на кожну конкретну дію чи перегляд об'єкта (наприклад, конкретного рецепта чи запису).

Також нагадаємо, що наразі тестування МІС на відповідність безпековим технічним вимогам проводиться під час кожного функціонального тестування МІС з видачею офіційного протоколу.