Захист персональних даних в сфері охорони здоров'я

Персональні дані пацієнтів у електронну систему вводяться, визначеними закладом охорони здоров'я уповноваженими особами, на яких поширюється дія законодавства про лікарську таємницю. Збір та обробка персональних даних пацієнта у системі «Електронне здоров'я» регулюється Законом України «Про захист персональних даних», Законом України «Про державні фінансові гарантії медичного обслуговування населення», Постановою Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я» № 411 від 25.04.2018.

Сама електронна система охорони здоров'я спроектована для роботи з персональними даними з дотриманням кращих світових практик у сфері захисту даних и знаходиться на серверах дата-центру в Україні, який має комплексну систему захисту інформації та пройшов атестацію у Державній службі спеціального зв'язку та захисту інформації. Від початку побудови електронної системи охорони здоров'я (ЕСОЗ) захист даних завжди був пріоритетним завданням. ЕСОЗ – одна з систем в Україні, в якій реалізовані найсучасніші засоби захисту, серед яких: використання користувачами кваліфікованих електронних підписів (КЕП), реалізація архітектурних принципів GDPR (відокремлене зберігання медичних та персональних даних), blockchain-подібні алгоритми, що забезпечують цілісність даних та інші. Так, лише на вході в систему користувачі проходять двофакторну авторизацію: через встановлену МІС та безпосередньо вхід в ЕСОЗ за протоколом OAuth.2.

Система має багаторівневий захист та отримала атестат відповідності комплексної системи захисту інформації.

Також кожен МІС, що підключений до ЦБД, повинен мати атестат відповідності комплексної системи захисту інформації (КСЗІ) відповідно до норм українського законодавства.

Ця вимога передбачена Законом України "Про захист інформації в інформаційно-комунікаційних системах" та іншими нормативно-правовими актами щодо підключення МІС до центральної бази даних ЕСОЗ.

Сьогодні наша держава бореться із загарбником на всіх фронтах і кіберфронт не є винятком. На рівні центральної бази даних адміністратор забезпечує проведення необхідних заходів із захисту інформації та попереджає реальні та потенційні атаки ворога.

Проте захист інформації також не менш важливий і на робочому місці кожного користувача. Для цього закладам охорони здоров'я необхідно:

- регулярно оновлювати програмне забезпечення (зокрема,операційних систем, систем керування базами даних, програмних бібліотек тощо);
- контролювати цілісність та автентичність ПЗ;
- забезпечувати мережевий захист: фільтрація та аналіз мережевого трафіку, виявлення і протидія мережевим атакам і т. д.;
- унеможливлювати втрату інформації, забезпечити резервне копіювання даних, захист від несанкціонованого доступу, розмежування прав доступу тощо;

- забезпечувати реєстрацію подій, пов’язаних з отриманням користувачами доступу до ресурсів ЗОЗ;

- проводити резервування конфігураційних файлів та критично важливих системних файлів;

- проводити перевірку кваліфікованого електронного підпису на інформаційних об’єктах в ЗОЗ її користувачами;

- забезпечувати антивірусний захист, перевірку на наявність шкідливого програмного коду всіх вкладень, що завантажуються користувачами до ЗОЗ.

Для забезпечення виконання всіх цих заходів доцільно в закладах охорони здоров’я визначити відповідальних за це осіб або ж створити відповідні ІТ підрозділи, а також забезпечити контакт таких осіб чи підрозділів зі службами підтримки медичних інформаційних систем, які працюють у закладі.