УДК 004.05+61

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕДИЦИНІ

Куперштейн Леонід, Войтович Олеся, Ясінська Яна

Вінницький національний технічний університет

Анотація

У даній роботі проведено загальний аналіз потенційних загроз інформаційної безпеці в сфері медицини. Актуальність тематики пояснюється низьким захистом медичних даних та частими випадками їх несанкціонованого витоку.

Abstract

In this work a general analysis of the potential threats to information security in the medicine is realized. The relevance of the topic is explained by the low protection of medical data and frequent cases of their unauthorized leakage.

Вступ

Протягом останніх років в Україні медичні установи активно переходять на електронний документообіг, автоматизується ведення електронного обліку або медичних карт пацієнтів [1]. З розвитком інформаційних технологій прискорився і перехід медичних установ на новий рівень обробки і зберігання персональних даних як співробітників, так і клієнтів. Ключова характеристика медичної інформації складається в необхідності забезпечення її конфіденційності. Персональні дані пацієнта, які вводяться і обробляються системою, складають основу лікарської таємниці [2]. Також важливим є те, що в інформаційних системах, найчастіше, зберігаються відомості, від цілісності та об'єктивності подання яких залежить не тільки здоров'я, а й життя людини. Багато документів потрапляють в категорію лікарської таємниці. Тому інформаційна безпека в медицині переходить на новий рівень. Таким чином, напрямки розробки та впровадження політики інформаційної безпеки (ПІБ) як розробки та експлуатації медичних інформаційних систем так і функціонування медичних закладів в цілому на сьогодні є досить важливими і актуальними.

Основна частина

Розробка ПІБ регламентується рядом нормативних документів, а саме: ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2013, ДСТУ ISO/IEC 27003-27006, НД ТЗІ 1.4-001-2000, положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України та ін. [3]. При розробці ПІБ, для будь-якої установи в тому числі і медичної, важливим етапом є оцінка стану інформаційної безпеки та визначення загроз для її ресурсів. Серед електронних інформаційних ресурсів медичної установи можуть бути дані баз даних та їх резервні копії, архівні копії ресурсів файлового сервера, керуюча інформація операційної системи, технологічний процес збору, обробки, зберігання та передачі інформації в медичній інформаційній системі, електронна документація тощо. Проте не менш важливими залишається і ряд не електронної документації, які також можуть бути вразливі до атаки.

Загрози, з якими можуть стикатись медичні установи – це зловмисні дії, людські помилки, збої в системі та мережеві поломки та природні явища [4]. Слід розглянути більш детально кожну з загроз.

1. Зловмисні дії – це навмисні дії особи чи організації. Особа, яка здійснює зловмисну дію, може бути зовнішньою (конкуренти, пацієнти, партнери) чи внутрішньою (співробітники) з боку постраждалої організації. Даний тип визначає низку загроз [5]: шкідливе програмне забезпечення (хробаки, трояни, руткіти, експлоїти, ботнети), викрадення даних, підробка медичного обладнання (перепрограмування); атаки на соціальну інженерію (фішинг, приманки), крадіжка даних через пристрої, скимінг, атаки відмов у наданні послуг тощо.

2. Помилки людини можуть трапитись ненавмисним чином під час конфігурації, експлуатації пристроїв чи інформаційних систем, а також під час виконання процесів. Ці помилки часто пов'язані з недостатньою кваліфікацією співробітників. Це можуть бути помилки конфігурації медичної системи, що може призвести до збою якихось певних операцій а то й всієї системи [4]. Ще однією загрозою є відсутність журналу аудиту для забезпечення належного контролю, що унеможливить виявлення інциденту. Ще однією загрозою цього типу є помилки лікаря та/або пацієнта, що може трапитись в результаті втоми і поганої концентрації через тривалий робочий час.

3. Збої в системі є надзвичайно актуальними в контексті охорони здоров'я, особливо через зростаючу складність та динаміку систем [2]. До них можна віднести збої в програмному забезпеченні, які впливають або повністю порушують медичний або адміністративний процес (наприклад, порушення доступності даних про пацієнта), поломка пристроїв або просто обмежена/знижена здатність можуть серйозно впливати на важливі процеси, наприклад, таких як збір даних в реальному часі про пацієнтів приладом для вимірювання глюкози, недостатнє технічне обслуговування, що може залишати невідкриті та невирішені експлуатаційні проблеми, а перевантаження може призвести до відмови певної послуги чи всієї системи.

4. Мережеві несправності знаходяться поза безпосереднім контролем постраждалої організації, оскільки це відбувається через відповідальність третьої сторони: хмарні постачальники послуг, виробники медичного обладнання, мережеві провайдери та постачальники електроенергії.

5. Природні явища також можуть бути причиною інцидентів, особливо через їх руйнівний вплив [5]. Більше того, природні явища можуть впливати на надання віддалених послуг з обслуговування пацієнтів, навіть якщо їх вплив не орієнтований або не впливає на саму лікарню, наприклад, землетруси; повені; пожежі.

Висновки

Як відомо немає універсального програмного забезпечення або технології, яка дозволить забезпечити стовідсотковий захист від потенційних загроз, проте важливо забезпечувати захист хоча б частково. Ризик кібератак наразі не є турботою лише IT відділів. В даний час – це ключове питання, яке має бути розглядатись керівництвом медичних установ. Сфері медичних послуг слід дбати про захист даних, пацієнтів, та про все що пов'язано з цією специфікою. Державі слід виділяти кошти на захист даних, задля забезпечення безпеки даних в медичних інформаційних системах.

Список використаних джерел

1.Информационная безопасность в медицинских информационных системах. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-sistemah/viewer (дата звернення: 02.05.2020).

2.Малышенко И.С., Бочко Е.К. Информационная безопасность в медицинских информационных системах // Сб. ст. по мат. XV междунар. студ. науч.-практ. конф. № 4(15). URL: https://sibac.info/archive/meghdis/4(15).pdf (дата звернення: 02.05.2020).

3.Куперштейн. Л.М., Ясінська Я.О. Дослідження політики інформаційної безпеки у розрізі нормативної документації // XLIX Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії (2020). URL: http://ir.lib.vntu.edu.ua//handle/123456789/29388 (дата звернення: 03.05.2020).

4.Cyber security and resilience for Smart Hospitals. URL: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals (дата звернення 01.05.2020).

5.Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки : навчальний посібник. Вінниця: ВНТУ, 2013. 221 с.