ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Ю.П. Гульчак

Вінницький національний медичний університет ім. М.І. Пирогова

м. Вінниця

Інформаційні ресурси медичного закладу є як продуктом діяльності персоналу, так і готовими об'єктами МІС, з якими працюють і до яких періодично повинні мати доступ окремі категорії спеціалістів. Важливим є забезпечення такого рівня захисту інформації, який би унеможливив захист її від несанкціонованого доступу, знищення, спотворення, копіювання, блокування тощо; захист апаратних і програмних компонентів МІС.

В Україні законодавчо закріплені класи автоматизованих систем за рівнем захищеності від несанкціонованого доступу, кожен з яких характеризується окремим набором елементів захисту, так званих профілів безпеки[1]. Загальна структура класу має вигляд X.YYY.Z (наприклад 2.КЦД.3), де X – функціональний клас АС (1,2,3), Y – підклас АС (К – конфіденційність, Ц – цілісність, Д - доступність), Z - функціональний профіль АС (1, 2, 3, 4, 5, 6).

В результаті аналізу ІС медичних установ різних рівнів рекомендовано: для сільських амбулаторій, лікарів приватної практики, інших закладів, які віднесені до АС класу 1 мінімально достатнім є стандартний профіль 1.КЦ.Z.

Для рівня первинної медичної допомоги основними загрозами є порушення конфіденційності інформації і, як результат, порушення її цілісності. Тому на початковому етапі достатньо запровадити прості профілі захисту АС класу 1; від 1.К.Z до 2.КЦ.Z для амбулаторій і 2.КЦ.Z для центрів ПМСД.

Для закладів вторинного і третинного рівнів з МІС на основі локальної мережі, рекомендовано профіль 2КЦ.Z (профілі з підвищеними вимогами до забезпечення конфіденційності і цілісності оброблюваної інформації).

Саме на цих рівнях зосереджена основна маса інформації, в якій зацікавлені потенційні порушники. Виходячи з цього доцільно в першу чергу забезпечити надійний захист баз персональних даних (зокрема історій хвороб) пацієнтів за напрямками конфіденційності та цілісності; захист баз даних службової медичної інформації, кадрової і бухгалтерської документації – за напрямком доступності. Крім того значно підвищуються вимоги до захисту інформації в телекомунікаційних мережах зв'язку при передачі великих масивів даних, так як телемедицина стає важливим елементом функціонування лікарні.

Рекомендовані вище профілі є базовими. Виходячи зі специфіки медичного закладу їх елементи можна змінювати, включаючи нові або змінюючи навіть підкласи захищеності оброблюваної інформації.

1. Гульчак Ю.П., Гульчак Е.Ю. Нормативно – правова база захисту інформації в медичній галузі. *Вісник Хмельницького національного університету.* 2018. №4. С. 194-203.