УДК 004.05+61

Ясінська Я. О.
Куперштейн Л. М.

РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕДИЧНОГО ЗАКЛАДУ

Вінницький національний технічний університет

Анотація

В даній роботі було досліджено етапи побудови політики інформаційної безпеки медичних закладів, проаналізовано кожен етап та надано рекомендації щодо його реалізації. Зазначається, що наразі є актуальним створення автоматизованої системи розробки політики безпеки організації.

Ключові слова: політика інформаційної безпеки, інформаційна безпека, захист інформації.

Abstract

This paper examines all stages of building an information security policy for medical institutions, analyzes each stage and provides recommendations for its implementation. It was also investigated that it is currently important to create an automated system for developing security policies of the organization.

Keywords: information security policy, information security, information protection.

Вступ

Інформаційні технології набувають все більшого і більшого поширення з кожним днем у всіх галузях, це стосується і медицини. Вони можуть забезпечити легкість та швидкість обробки потрібної інформації у потрібний час, але при цьому мають побічний ефект такий, як: ризик інформаційної безпеки.

Медична інформація має високу цінність для зловмисників, так як її ціна на чорному ринку є найвищою, саме тому відома велика кількість випадків, коли така інформація була викрадена чи виставлена для загального бачення. Тому постає необхідність в захисті інформації в сфері охорони здоров'я, та забезпечення їй цілісності, доступності та конфіденційності. Для реалізації високого рівня захисту в організації необхідним є розробка та впровадження політики інформаційної безпеки (ПІБ), яка являє собою сукупність документованих рішень, які приймаються вищим керівництвом організації та спрямовуються на захист інформації та асоційованих з нею ресурсів [1, 2].

Побудова політики інформаційної безпеки

Побудова ПІБ будь-якої організації, а в тому числі і для медичних установ, включає в себе наступні етапи: аналіз об'єкту захист; ідентифікація цінних активів; аналіз загроз для досліджуваного об'єкту; оцінка ризиків; створення правил, рекомендацій, вимог, спрямованих на захист установи.

Аналіз об'єкту захисту, тобто медичного закладу, полягає у дослідженні фізичного середовища об'єкта, інформаційного середовища та середовища користувачів. На даному етапі також слід дослідити організаційну структуру цього закладу.

Ідентифікація цінних активів полягає у досліджені ресурсів об'єкта захисту. Згідно з ДСТУ ISO/IEC 27005:2019 активи організації поділяються на [3]: інформацію, апаратно-програмний комплекс, носії інформації, мережа, персонал, місце функціонування організації. Кожен актив оцінюється за 4-х бальною шкалою. Це допоможе визначити найбільш важливі та критичні ресурси.

Ідентифікація загроз зазвичай проводиться експертним підходом, так як відсутня статистика. Експертні оцінки можна формалізувати за допомогою теорії нечітких множин. Даний метод дозволяє визначити найбільш точну ймовірність виникнення події. Формалізація передбачає два етапи: – фазифікацію (розмиття) та дефазифікацію (отримання найбільш достовірного значення) [4]. Найбільш поширеними загрозами для медичних закладів є: зловмисні дії, людські помилки, збої в системі та мережеві поломки та природні явища [5]. Оцінка ризиків організації повинна здійснюватися згідно з вимогами ДСТУ ISO/IEC 27001:2013 на основі даних отриманих з вищевказаних етапів.

Останнім етапом є створення власне політики інформаційної безпеки. Оскільки за Законом Украї-

ни «Про основні засади забезпечення кібербезпеки України» (стаття 6, пункт 2) медичні установи відносяться до об’єктів критичної інфраструктури (ОКІ), то ПІБ повинна відповідати вимогам Постанови КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [6]. За цією Постановою ПІБ повинна складатись з 18-ти розділів. ПІБ повинна враховувати оцінку ризиків та спрямовувати захист на найбільш вразливі місця.

Так, як структура ПІБ є визначеною для усіх медичних установ, то є актуальним – створення автоматизованої системи розробки політики безпеки організації. Дана система вимагатиме від користувача обрати зі списку доступних активів (ЦА) ті, які притаманні його організації. Потім користувачу надається матриця рівня вразливості загроз, в якій він сам повинен задати рівень вразливості (РВ), у відповідності кожного активу до кожної загрози. Далі користувач задає ймовірність реалізації загрози (ЙЗ), після чого виконується оцінка ризиків за формулою:

$$Р = ЦА \times РВ \times ЙЗ$$

На основі цих оцінок підбираються контрзаходи, на основі яких формується документ у вигляді ПІБ. Це дозволить за короткий час створити основу загальної ПІБ організації на основі відомих даних про неї та при необхідності доповнити необхідними матеріалами [7].

Висновки

Проаналізовано етапи створення політики інформаційної безпеки, розглянуто більш детально кожен етап та визначено кроки, які необхідно на них виконати. Визначено, що медичні установи відносяться до об’єктів критичної інфраструктури, тому мають особливості щодо змісту політики інформаційної безпеки. Для спрощення процесу розробки ПІБ запропоновано функціонал автоматизованої системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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

2. Куперштейн. Л.М., Ясінська Я.О. Дослідження політики інформаційної безпеки у розрізі нормативної документації. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/29388/9339.pdf?sequence=3 (дата звернення 12.12.2020).

3. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки / Нац. стандарт України. – Вид. офіц. – [Чинний від 2019-11-01]. – Київ : ДП «УкрНДНЦ», 2019. – 76 с.

4. Дудатьев. А. В., Лужецкий В. А., Коротаев В. А.. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны. Україна: Харків, 2016. 4-11 с. URL: http://nbuv.gov.ua/UJRN/ Vejpte_2016_2%282%29__2 (дата звернення: 14.12.2020).

5. Куперштейн Леонід, Войтович Олеся, Ясінська Яна. Аналіз загроз інформаційної безпеки в медицині. URL: https://ir.lib.vntu.edu.ua/ bitstream/handle/123456789/30909/WORK-IES-2020-242-243.pdf?sequence=1 (дата звернення: 15.12.2020).

6. Про основні засади забезпечення кібербезпеки України: Закон України від 17.09.2020 № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20201024#Text (дата звернення 16.12.2020).

7. Азарова А. О., Карпінець В. В. Методичні вказівки до проведення прктичних занять та до виконання самостійної й індивідуальної роботи з дисципліни «Основи науково-дослідної роботи»: методжичні вказівки. Вінниця: ВНТУ, 2013. 44 с.

Ясінська Яна Олександрівна – студентка групи 1БС-20м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: yankayasinskaya.7@gmail.com.

Куперштейн Леонід Михайлович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Yasinska Y. – Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: yankayasinskaya.7@gmail.com.

Kupershtein L. – PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, Ukraine.