УДК 004.05+006.4

Л. М. Куперштейн
Я. О. Ясінська

ДОСЛІДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У РОЗРІЗІ НОРМАТИВНОЇ ДОКУМЕНТАЦІЇ

Вінницький національний технічний університет

Анотація

В даній роботі було розглянуто поняття політики інформаційної безпеки в межах нормативних документів. Досліджено стандарти ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2013. Досліджено принцип розробки політики інформаційної безпеки, як одного з етапів створення комплексної системи захисту інформації за НД ТЗІ 1.4-001-2000. Розглянуто поняття політики інформаційної безпеки в положенні про організацію заходів із забезпечення інформаційної безпеки в банківській системі України.

Ключові слова: Політика інформаційної безпеки, захист інформації, нормативна документація.

Abstract

In this paper, the concept of information security policy within the framework of regulatory documents was considered. The following standards of ISO / IEC 27001: 2015, ISO / IEC 27002: 2013 have been investigated. The principle of development of information security policy as one of the stages of creation of a comprehensive system of information protection by RD TPI 1.4-001-2000 is investigated. The concept of information security policy in the provision on organization of information security measures in the banking system of Ukraine is considered.

Keywords: Information security policy, information security, regulatory documentation.

Вступ

Інформація з кожним днем стає все більш цінним ресурсом для будь-якого підприємства чи установи. Для її повного захисту потрібні певні правила для роботи з цією інформацією та для її обробки. Дані правила, як відомо, прописуються в документі, що має назву «Політика інформаційної безпеки» (ПІБ)[1]. Вона є невід'ємною частиною будь-якої «захищеної» установи та являє собою систематизований виклад цілей і завдань захисту даної установи, якими необхідно керуватися в своїй діяльності кожному співробітнику. Актуальністю даної статі є застосування поняття ПІБ в різних стандартах та нормативних документах. Метою статті є порівняльний аналіз вимог до розробки ПІБ в нормативно-методологічній базі.

Основна частина

Під політикою безпеки інформації розуміється набір вимог, правил, обмежень, рекомендацій та ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз [1, 2].

За стандартом ДСТУ ISO/IEC 27001:2015 визначається, що ПІБ будь-якої установи передбачає її впровадження вищим керівництвом цієї установи. Також дана ПІБ повинна [3]:

- відповідати цілям організації;
- містити цілі інформаційної безпеки або зазначати основні положення для визначення цілей інформаційної безпеки;
- містити зобов'язання відповідати застосованим вимогам, пов'язаним з інформаційною безпекою;
- містити зобов'язання щодо постійного вдосконалення системи управління інформаційною безпекою.

За цим ж стандартом передбачається, що розроблена ПІБ повинна бути доступною як документована інформація, бути розповсюдженою в середині організації та бути доступною зацікавленим сторонам, за потреби.

За ДСТУ ISO/IEC 27002:2013 завдання ПІБ полягає в забезпеченні орієнтації менеджменту і підтримки інформаційної безпеки в відповідності з вимогами бізнесу та відповідними законодавчими і нормативними вимогами [4]. За цим документом ПІБ має два рівні – верхній та нижній. На вищому

рівні організація повинна сформулювати «політику інформаційної безпеки», яка схвалена менеджментом і визначає підхід організації до управління досягнення цілей в галузі безпеки.

На нижньому рівні політика інформаційної безпеки повинна розкриватися в політиках за відповідними напрямами, які далі реалізуються в засобах управління інформаційною безпекою та, як правило, поділяються відповідно до потреб певних цільових груп в організації або за певними цільовими областям.

Поняття ПІБ застосовується також у таких стандартах, як ДСТУ ISO/IEC 27003-27006, де вказується, що вона є важливим аспектом кожної організації та повинна відповідати вимогам зазначеним у ДСТУ ISO/IEC 27001:2015.

ПІБ важлива для усіх організацій та установ, та особливо важлива для банківських систем. В положенні про організацію заходів із забезпечення інформаційної безпеки в банківській системі України зазначено, що банк зобов'язаний розробити та впровадити політику інформаційної безпеки, яка має містити [5]:

- цілі інформаційної безпеки;
- сферу застосування політики інформаційної безпеки;
- принципи, правила та вимоги інформаційної безпеки в банку;
- визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки.

Також за даним документом передбачається, що банк зобов'язаний забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік. Якщо за результатами перегляду зміни до політики інформаційної безпеки не вносяться, то повторне її затвердження не потрібно.

Крім того, розробка ПІБ є одним з етапом створення комплексної системи захисту інформації (КСЗІ). За НД ТЗІ 1.4-001-2000 методологія розробки ПІБ включає в себе наступні роботи [6]:

- розробка концепції безпеки інформації в АС;
- аналіз ризиків;
- визначення вимог до заходів, методів та засобів захисту;
- вибір основних рішень з забезпечення безпеки інформації;
- організація виконання відновлювальних робіт і забезпечення неперервного функціонування АС;
- документальне оформлення політики безпеки.

Висновки

Проаналізовано поняття «політика інформаційної безпеки» на його місце у нормативній документації. Визначено, що вона є необхідним заходом для забезпечення безпеки організації. Досліджено, що для розробки ПІБ за будь-яким стандартом спочатку потрібно визначити цілі безпеки – на, що повинна спрямовуватись безпека. В ряді нормативних документів зазначається, що при існуванні ПІБ в організації кожен співробітник зобов’язаний дотримуватись її правил, у разі невиконання яких можуть застосовуються різні методи стягнень та покарань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.

2. Політика інформаційної безпеки: мета, задачі та основний зміст [Електронний ресурс]. – Режим доступу: URL https://studfile.net/preview/2265905/ - Назва з екрану.

3. ДСТУ ISO/IEC 27001:2015. Методи захисту системи управління інформаційною безпекою.

4. ДСТУ ISO/IEC 27002:2013. Звід правил для управління інформаційною безпекою.

5. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс]. – Режим доступу: URL https://zakon.rada.gov.ua/laws/show/v0095500-17 – Назва з екрану.

6. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затв. наказом ДСТСЗІ СБУ від 04.12.2000 р. №53.

Ясінська Яна Олександрівна – студентка групи 1БС-16б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: yankayasinskaya@ukr.net .

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@ukr.net .

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