Гришко С.В.
к.е.н., доцент кафедри економічної кібернетики
та управління економічною безпекою,
Харківський національний університет радіоелектроніки
Кодрул Р.Е.
студент,
Харківський національний університет радіоелектроніки

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ОРГАНІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Інформаційна безпека представляє набір інструментів та методів для захисту різних видів інформації. Вона включає безліч сучасних інформаційних технологій, використання яких стає необхідністю успішного функціонування підприємств. Загалом під інформаційною безпекою розуміється стан інформаційного середовища, який забезпечує розвиток цього середовища, ефективне використання інформації в інтересах підприємства, а також захищеність від будь-яких загроз [1]. Забезпечення інформаційної безпеки на підприємстві слід розглядати як невід'ємний елемент процесу управління підприємством [2].

Застосування СУІБ (Система управління інформаційною безпекою) є однією з умов розвитку бізнесу, її використання при виникненні загроз інформаційним системам підприємства забезпечує спроможність до протистояння загрозі та подальшого існування. Використовуючи методи ризик-менеджменту, а також застосування інших процедур, організаційних методів, програмного та технічного забезпечення, досягається реалізація інформаційної безпеки підприємства.

Процедури для реалізації системи управління інформаційною безпекою можуть бути організовані як дерево процесів [3]. Створення ефективної

системи управління інформаційною безпекою можна описати певною послідовністю заходів на підприємстві, така послідовність може включати етапи (рис. 1), фактична реалізація яких залежить від специфіки конкретного підприємства. Етапи формування визначають впровадження заходів, виконання певних дій або прийняття рішень, які можна поділити на три блоки. Перший та другий етап забезпечують встановлення сфери застосування СУІБ. З третього по сьомий етапи відбувається впровадження захисних заходів на основі ризик-менеджменту. Етапи 8-10 зазначають процеси схвалення керівництвом рішень для впровадження засобів обробки ризиків, формулювання вимог, та дозволів на реалізацію та використання механізмів системи.

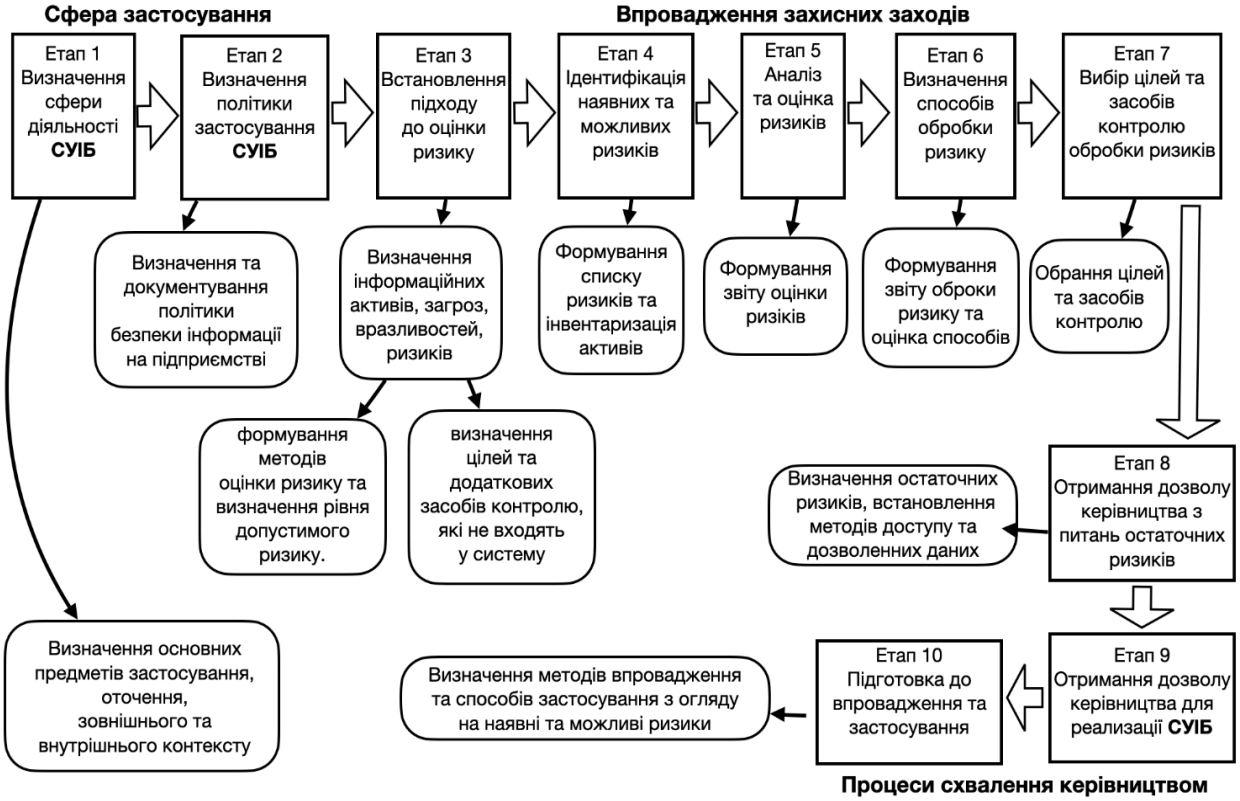

Рисунок 1 – Послідовність формування системи управління інформаційною безпекою на підприємстві

Джерело розроблено на основі [3]

Ураховуючи велику кількість процесів інформаційної безпеки під час діяльності підприємства, ефективна СУІБ повинна враховувати засоби призначені для розробки, впровадження, функціонування, моніторингу,

перегляду, підтримування, а також розвитку та вдосконалення інформаційної безпеки [2]. Також важливо враховувати вже напрацьовані стандарти, які допоможуть реалізувати ефективну у використанні систему, такі стандарти, пропонують сформовані вимоги до побудови, методи використання та засоби розвитку СУІБ на підприємстві.

Таким чином, системи управління інформаційною безпекою є невід'ємною частиною загального управління підприємством, вони забезпечують стійкість інформаційних структур до внутрішніх та зовнішніх загроз а також дозволяють впроваджувати заходи щодо розвитку, завдяки можливості прогнозувати стан підприємства відносно можливих загроз. Великий досвід застосування міжнародних стандартів формування систем управління інформаційною безпекою підприємства, який базується на основі менеджменту ризиків, дозволяє будувати системи, які спроможні захищати підприємство та забезпечувати його розвиток. Треба також зазначити, що під час реалізації інформаційної безпеки перед підприємством постає задача у пошуку ефективного балансу між відповідністю системи та її засобів конкретному підприємству, зручністю використання та рівнем забезпечення безпеки інформації.

Перелік джерел посилання

1. Кавун С. В., Пилипенко А. А., Ріпка Д. О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації. *Навчальний посібник. Вид. ХНЕУ*. 2013. 364 с.

2. Якименко Ю. М., Мужанова Т. М., Легомінова С. В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. № 4(12). С. 36-50.

3. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*. 2016. 3(1). 80 с.