УДК 004.056

***Чайкіна Аліна Олександрівна*[6],**
кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА ЯК ОСНОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ РЕГІОНУ

Регіональний розвиток залежить від багатьох факторів, по-перше, від сформованої політики органів державної влади щодо підтримки громади, бізнесу, по-друге, від системи взаємодії усіх стейкголдерів у нарощенні та реалізації потенціалу регіону, формування його конкурентних переваг, а також від політики протекціонізму, коли в першу чергу підтримується власний виробник, який задовольняє попит населення. Проте сьогодні додається ще один із напрямів забезпечення економічної безпеки та загалом сталого розвитку регіону чи країни – це інформаційна безпека, яка передбачає створення комплексу правових, технічних і організаційних заходів, що спрямовані на запобігання неправомірних дій з інформацією на всіх рівнях від рівня звичайного громадянина до рівня держави.

Загалом систему управління інформаційною безпекою розуміють як частину загальної системи управління, яка аналізує ризики і загрози, створює, реалізує, контролює та вдосконалює заходи у сфері інформаційної безпеки. Можна виділити наступні проблеми, які постають перед учасниками у сфері інформаційної безпеки:

[6] Тези підготовлено в межах виконання НДР молодих учених «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди», державний реєстраційний номер 0124U000615

підтримка високого рівня інформаційної безпеки;

зовнішні та внутрішні канали витоку інформації;

грошові втрати від настання кризових ситуацій;

атаки на інформаційну базу;

недосконаліть програмного забезпечення та використання неліцензованих програм, застосунків;

персональні мобільні пристрої, що мають доступ до акаунтів з конфіденційною та персональною інформацією [1].

З метою створення ефективної системи інформаційної безпеки важливо дотримуватися низки ключових принципів:

комплексність та узгодженість, коли відбувається активна взаємодія на всіх рівнях, починаючи від затвердження нормативно-правового поля і завершуючи контролем виконання усіх вимог захисту;

побудова системи захисту інформації, яка передбачає застосування конкретних інструментів та методів захисту;

диференціація – рівні захисту мають розроблятися з урахуванням важливості та критичності інформації, оцінки потенційних атак;

достатність механізмів захисту – передбачає оцінку співвідношення витрат на створення та підтримку системи захисту інформації від можливої шкоди.

Саме тому важливим є питання економічного обґрунтування витрат на захист інформації, адже чим вище рівень захищеності інформації, тим буде нижче розмір можливих збитків, але вищою буде вартість впровадження такого захисту. Багато підприємств не готові витрачати кошти для побудови ефективної інформаційної системи протидії ризикам і загрозам, звертаючись до неї вже після настання кризової ситуації. Оптимальний розміром витрат на захист буде такий, при якому забезпечується рівень захищеності, що дорівнює мінімуму загальних витрат. Вартість збитків визначається двома параметрами: ймовірністю реалізації різних загроз інформації; вартістю (важливістю) інформації,

захищеність якої може бути порушена під впливом різних загроз.

Отже, в сучасних умовах, без належного захисту інформаційного середовища підприємства не можливо забезпечити ні його економічну безпеку, ні безпеку регіону [2]. Саме тому на регіональному рівні мають бути створенні спеціальні центри, які будуть допомагати у виборі правильного програмного забезпечення, надаватимуть пільги або грантове фінансування підприємствам, які здійснюють свою діяльність для забезпечення економічної, соціального та екологічної безпеки регіону.

Стандарти управління інформаційної безпеки повинні відігравати важливу роль в цьому відношенні. Менеджмент підприємства реалізує компоненти безпеки інформації, такі як політика і технічні заходи безпеки, з якими працюють їх співробітники, впроваджує прийнятний рівень культури безпеки інформації, створює єдину систему інформаційної безпеки, ефективно реалізовує всі необхідні компоненти інформаційної безпеки [3]. Підтримкою в цьому процесі повинен бути спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації [4], який має надавати всебічну підтримку таким підприємствам, розробляти пропозиції щодо проведення спеціальних тренінгів, просвітницьких кампаній для менеджменту підприємства з кібербезпеки, надавати доступ до певних державних інформаційних ресурсів з метою активної взаємодії учасників процесу інформаційного захисту, контролювати за використанням ліцензованого програмного забезпечення підприємствами, дотримання прав інтелектуальної власності, виявляти загрози державним та приватним інформаційним ресурсам від несанкціонованих дій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах тощо.

Отже, підвищуючи рівень інформаційної безпеки підприємств та всебічна підтримка з боку державних органів влади щодо створення ефективної системи протидії кібератакам та несанкціонованому доступу до мереж, припинення використання неліцензійного програмного забезпечення, проведення тренінгів для менеджерів щодо підвищення їх компетенції у сфері інформаційної безпеки дозволить забезпечити захист інтересів держави і суспільства, підвищить конкурентоспроможність регіону, його економічний розвиток. Лише при активній взаємодії на всіх рівнях можливо осягнути сталого розвитку регіону, захистити інтереси бізнесу і надалі реалізовувати соціально значущі проєкти для громади.

Література

1. Русіна Ю. О., Острякова В. Ю. (2017). Удосконалення системи управління інформаційною безпекою на підприємстві. Міжнародний науковий журнал Інтернаука, (14), 135-139.

2. Шевченко С. Ю., Шевченко С. Ю. (2012). Формування системи управління інформаційної безпеки підприємства.URL: https://ir.kneu.edu.ua/bitstream/handle/2010/9137/329-331.pdf?sequence=1

3. Каркавчук В., Черчук А. (2015, October). Оптимізація управління інформаційною безпекою підприємства. In International Scientific Conference" Problems of Information Economy Formation in Ukraine, p. 190.

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

5. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association*. 2023. 29(5). pp . 818–835.