додаткові риски для зарубіжних торгових партнерів. Ці риски значно зростають при непередбачуваних, дискримінаційних і заборонних протекціоністських заходах, особливо що приймаються урядами порушуючи загальноприйняті міжнародні правила і зобов'язання. [2]

Таким чином, очевидно, що облік і аналіз можливих ризиків також є невід'ємною і украй важливою складовою управління зовнішньоторговельною діяльністю підприємства в умовах виходу на зовнішній ринок. Більше того без ефективної системи управління рисками не можливо і реалізація ефективної зовнішньоторговельної стратегії підприємства.

Література

1 Пелагеша Н.Є. Трансформація української національної ідентичності під впливом глобалізації //Віче. - 2007. - № 18. - С. 55-56.

2 Ягубов Ш. Р. Ризики підприємств на глобальному ринку // Вестник Саратовского государственного социально-экономического университета. 2008. №5. URL: http://cyberleninka.ru/article/n/riski-predpriyatiy-v-globalnom-rynke (дата обращения: 05.04.2017).

Тарасова К.І.,
к.е.н., викладач кафедри статистики
Одеського національного економічного університету

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ

Малі та середні підприємства (МСП) є важливою частиною економічної та інформаційної інфраструктури України. Згідно з даними Державної служби статистики, на нашому ринку функціонує понад 343 тис. МСП, які виробляють 77,8 % реалізованої продукції та створюють 75,8 % робочих місць [1].

Для більшості МСП безпека інформаційних систем має низький пріоритет. Проте, за останні десятиліття неконтрольоване використання кібернетичного простору призвело до уразливості даних для стороннього впливу. Порушення інформаційної безпеки може мати згубні наслідки для клієнтів, співробітників та партнерів МСП, а також для самого їх бізнесу. Дуже важливо, щоб кожне підприємство розуміло та управляло ризиками даних, систем і мереж, які підтримують їх функціонування [2].

Сьогодні багато компаній спрямовують свої ресурси, в тому числі людей, технології та гроші, на захист від загроз інформаційних та кібернетичних ризиків. В результаті, вони стають більш важкою мішенню для атак з боку хакерів, а самі злочинці звертають свою увагу на менш захищені об’єкти.

Малі та середні підприємства, на відміну від великих компаній, не мають достатньо коштів для інвестування в інформаційну безпеку, що робить їх легкими

цілями для шахрайства [3]. У 2016 р. світова вартість реалізації кібер-ризиків, найбільший тягар якої понесли одні із провідних економік світу, склала 445 млрд. доларів (табл. 1).

Таблиця 1 Вартість кібер-ризиків та уразливості інформаційної системи для провідних економік у 2016 р.

Назва країни	Розмір збитку для економіки, млрд. дол.	Розмір кібер-ризику у % до ВНП
Усього	445,0	…
у т.ч.		
США	108,00	0,64
Китай	60,00	0,63
Німеччина	59,00	1,60
Бразилія	7,70	0,32
Великобританія	4,30	0,16
Індія	4,00	0,21
Франція	3,00	0,11
Росія	2,00	0,10
Японія	0,98	0,20
Італія	0,90	0,04

Варто відзначити, що злочинці не завжди націлені на прибуток підприємства. МСП може мати корисну для хакера інформацію; комп'ютер може бути зламаний та використаний для атаки когось іншого; або бізнес може забезпечити доступ до цілей більш високого профілю через свої товари, послуги або ролі в ланцюжку постачання.

Загальний негативний ефект від кібер-інцендентів також може включати втрату прибутку, неможливість отримати банківський кредит, пошкодження інформаційної системи, зниження продуктивності, втрату репутації проміж клієнтів.

Нажаль, в цьому відношенні, МСП часто мають більше втрачати, ніж великі підприємства тому що кібер-атака буває надзвичайно коштовною. Малі та середні підприємства менш спроможні справлятися з такими подіями, але існує і багато кроків, які вони можуть зробити для покращення своєї ситуації з інформаційною безпекою.

МСП часто розглядають інформаційну безпеку як занадто важку, що вимагає багато ресурсів. Проте, якщо сприймати її як частину бізнес-стратегії, вона стане більш прийнятною.

Дії з співвідношення інформації та відповідного їй захисту називаються інформаційним ризик-менеджментом. Для того, щоб бути успішним, цей процес вимагає взаємодії широкого кола персоналу підприємства. Також необхідно переглядати та оновлювати план із управління ризиками хоча б раз на рік або під час значних змін у веденні бізнесу (наприклад, на початку нового проекту чи при зміні ІТ-системи).

Вчені-спеціалісти в сфері економічної безпеки та ІТ-технологій підрозділяють процес менеджменту інформаційної безпеки на декілька етапів [4]:

1. Визначення типу інформації, яку зберігає та використовує МСП. Цей перший крок часто є найбільш складною та найбільш важливою частиною управління ризиками.

2. Оцінка вартості інформації за критеріями конфіденційності, цілісності та доступності. На цьому етапі варто провести ранжування даних в залежності від ступеня їх значимості.

3. Складання інвентарного списку. Цей крок передбачає встановлення відповідності між інформацією, якою володіє МСП, та технологіями, які використовуються для зберігання, обробки та передачі цієї інформації.

4. Аналіз загроз та вразливостей інформаційній безпеці МСП. Підприємець повинен регулярно перевіряти, з якими загрозами може зіткнуся його бізнес і оцінювати можливі збитки.

5. Вибір засобів захисту від кібер- та інформаційних ризиків. Для кожного типу даних існує багато таких методів, а найбільш поширеними з них є: обмеження доступу співробітників до інформації, установка пристроїв захисту від перенапруг та безперебійного живлення, установка і активація програмного забезпечення та апаратних брандмауерів на всіх бізнес-мережах, налаштування веб-фільтрів і фільтрів електронної пошти, використання шифрування для чутливої ділової інформації, безпечна утилізація старої техніки тощо.

Щоденна життєва практика переконливо доводить, що забезпечення інформаційної та кібернетичної безпеки – процес безперервний, надзвичайно складний і багатогранний. Стратегічним завданням підприємства має стати формування комплексної системи менеджменту інформаційної і кібернетичної безпеки, в основу якої покладено організаційні аспекти функціонування підприємства.

Література:

1. Державна служба статистики України [Електронний ресурс]. – Режим доступу :http://www.ukrstat.gov.ua. – Назва з екрану.

2. Підгорний А. З. Статистичні методи в управлінні розвитком регіону : монографія // А. З. Підгорний, О. В. Самотоєнкова, О. Г. Милашко та ін. – Одеса : ФОП Гуляєва В. М., 2016. – 218 с.

3. Global Economic Prospects. June 2016. Divergences and Risks [Electronic resource]. – 2016. – № 26. – Available at: http://pubdocs.worldbank.org/en/842861463605615468/Global-Economic-Prospects-June-2016-Divergences-and-risks.pdf (date of appeal: 14.03.17). – Title screen.

4. Small Business Information Security: *The Fundamentals* [Electronic resource]. – 2016. – Available at: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf(date of appeal: 14.03.17). – Title screen.