Management in the Era of Globalization: Conference Proceedings. January 29, 2016. Klaipeda: Baltija Publishing. 270-271 p.

4. Вітлинський В. В. Системне використання об'єктивних і суб'єктивних показників ризику у фінансово-економічній сфері. *Фінанси України.* 2000. № 12. С. 16-24.

5. Ганущак Т. В. Методи управління фінансовою безпекою підприємства / Т. В. Ганущак// Наука й економіка. 2012. № 3 (27). С. 13- 17.

Низюк Є.М., студентка
Науковий керівник: Борисюк О.В.,
к.е.н., доцент
Східноєвропейський національний
університет ім. Лесі Українки, м. Луцьк, Україна

ВНУТРІШІ ТА ЗОВНІШНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В МОВАХ НЕОІНДУСТРІАЛЬНОГО СУСПІЛЬСТВА

Пріоритетним напрямком у процесі формування та забезпечення інформаційної безпеки будь-якої компанії є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Це, природно, вимагає конкретних дій, спрямованих на захист інформації з обмеженим доступом. Як свідчить вітчизняна і закордонна преса, кількість злочинів в інформаційній сфері не тільки не зменшується, але й має досить стійку тенденцію до росту.

Зовнішні загрози - це такі загрози, джерела яких знаходяться поза системою. До зовнішніх загроз інформаційної безпеки підприємства можна віднести: а) промислове і економічне шпигунство, шантаж, дезінформацію, атаки на систему захисту з метою крадіжки, знищення, спотворення інформації, підриву нормальної роботи підрозділів; б) відсутність на ринку достатньої кількості сертифікованих засобів захисту інформації; неповноцінність існуючої нормативно-правової бази інформаційної безпеки; в) діяльність недобросовісних партнерів, клієнтів [2, С. 9].

Внутрішні загрози інформаційної безпеки підприємства - це такі загрози, джерела яких розташовуються усередині системи. До внутрішніх загроз інформаційної безпеки підприємства можна віднести: а) застарілі програмно-технічні засоби зберігання і обробки даних; б) недосконаліть використовуваної системи захисту інформації; в) використання «піратського» програмного забезпечення; саботаж персоналу; г) низьку кваліфікацію співробітників; д) недостатню пожежну, технічну безпеку приміщень, будівель підприємства.

Система забезпечення інформаційної безпеки організації розглядається як цілий комплекс прийнятих управлінських рішень, спрямованих на виявлення і запобігання зовнішнім та внутрішнім загрозам. Ефективність вжитих заходів ґрунтується на визначенні таких факторів, як ступінь і характер загрози,

аналітична оцінка кризової ситуації і розгляд інших несприятливих моментів, які становлять небезпеку для розвитку підприємства і досягнення поставлених цілей.

Основна мета забезпечення комплексної системи інформаційної безпеки для захисту підприємства - це створення сприятливих умов для нормального функціонування в умовах нестабільного середовища; забезпечення захисту власної безпеки; можливість на законний захист власних інтересів від протиправних дій конкурентів; забезпечення співробітників збереженням життя і здоров'я; запобігання можливостей матеріального і фінансового розкрадання, спотворення, розголошення та витоку конфіденційної інформації, розтрати, виробничих порушень, знищення майна і забезпечення нормальної виробничої діяльності [2, с. 15].

Для того, щоб система забезпечення інформаційної безпеки організації діяла вона повинна ґрунтуватися на наступних принципах:

1) принцип комплексності, тобто при створенні систем захисту інформації повинна бути передбачена можливість виникнення всіх можливих загроз для конкретної організації. Використовувані засоби захисту повинні збігатися з імовірними видами загроз і функціонувати комплексно, доповнюючи один одного технічно;

2) принцип безперервності, тобто робота всіх систем безпеки повинна бути безперервною і цілодобової;

3) принцип надійності, тобто всі зони безпеки повинні мати однаковий ступінь надійного захисту;

4) принцип ешелонування, тобто забезпечення інформаційної безпеки організації буде здійснюватися в такому порядку, при якому всі зони системи захисту інформації будуть розташовуватися послідовно, а найважливіша з них буде розташовуватися всередині всієї системи;

5) принцип розумної достатності, тобто застосування захисних засобів має бути розумним без спроб створення «абсолютного захисту». Потрібно розуміти, що ефективні системи захисту інформації дуже дорогі, тому до їх вибору необхідно підходити раціонально. Вартість захисної системи не повинна перевищувати розмір можливого збитку і витрат на її обслуговування та функціонування [1, С. 5].

Водночас захист інформації повинен здійснюватися комплексно, відразу по декількох напрямках. Чим більше методів буде задіяно, тим менша ймовірність виникнення загроз і витоку, і тим стійкіше положення компанії на ринку.

Отже, в умовах розвитку неоіндустріальної економіки моніторинг інформаційної безпеки на підприємстві полягає в постійному контролі за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм, самотестування).

Список використаних джерел:

1. Литвиненко О. Інформація і безпека. *Нова політика*. 1998. № 1. С. 47–49.

2. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т. Шевченка.* 1999. Вип. 14. С. 46–48.
3. Борисюк О. В. Основні загрози фінансової безпеки України. *International Scientific-Practical Conference Modern Transformation of Economics and Management in the Era of Globalization*: Conference Proceedings. January 29, 2016. Klaipeda: Baltija Publishing. 270-271 p.
4. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету* 2010. № 2. Т. 2. С. 32–35.
5. Карлін М. І. Борисюк О. В. Управління державними фінансами: посібник / М.І. Карлін, О. В. Борисюк. Луцьк : ПП ІванЯчук, 2013. 273 с.
6. Крюков О.І. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво.* 2007. № 2. Режим доступу: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12.

Пархомчук Ю.А., студент
Шостак Л.В.,.к.е.н., доцент
Східноєвропейський національний
університет ім. Лесі Українки, м. Луцьк, Україна

ЗАГРОЗИ ФІНАНСОВО-ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Ефективність та стабільність економічної системи національної економіки значною мірою залежать від рівня фінансово-економічної безпеки підприємств. Водночас рівень фінансово-економічної безпеки підприємств перебуває під постійним впливом як внутрішніх, так і зовнішніх загроз, серед яких, передусім, необхідно виділити економічну нестабільність у державі. Наслідки таких проявів суттєво відбиваються на показниках фінансового стану підприємств, що, в свою чергу, призводить до зниження рівня їх фінансово-економічної безпеки. Виходячи з цього, зростає актуальність здійснення управління фінансово-економічною безпекою підприємств в умовах економічної нестабільності. Наслідки такого управління позитивно відобразяться не тільки на рівні фінансово-економічної безпеки підприємств, а й на строках стабілізації економіки.

Важливість забезпечення та підтримки фінансово-економічної безпеки підприємства на максимально можливому рівні не піддається сумніву. Проте досягти цього можна, лише системно підійшовши до цього питання. По-перше, діяльність з управління фінансово-економічною безпекою підприємства має здійснюватися постійно та безперервно. По-друге, процес управління має базуватися на складній та багатоступінчастій системі забезпечення управління фінансовою безпекою підприємства. Саме тому успішність і ефективність процесу забезпечення управління фінансово-економічною безпекою підприємства значною мірою залежать від досконалості та злагодженості взаємодії елементів покладеної в його основу системи. В свою чергу, лише ретельне вивчення науково-теоретичних засад побудови такої системи та використання цих знань при практичній розробці останньої може забезпечити її досконалість та ефективність.

Сучасна економічна система несе безліч загроз та небезпек економічній безпеці як економіки України, так і окремим підприємствам зокрема. Причому, не варто ліквідовувати відкритість економіки, а варто зосередити окрему частину