Джерела та література

1. Міжнародна конвенція про підготовку та дипломування моряків та несення вахти (ПДНВ) 78/95.
2. Алексишин Б. Г. Международные и национальные стандарты безопасности мореплавания. Одесса: Латстар, 2002. 256 с.
3. Топалов В. П., Торский В. Г. Маркетинг и менеджмент в судоходстве (основные понятия, элементы и принципы): учеб. пособие. Одесса: Астропринт, 2008. 84 с.

Низюк Є. − студентка

Науковий керівник: к. е. н., доц.
О. Борисюк
Волинський національний
університет імені Лесі Українки
м. Луцьк, Україна

Принципи забезпечення інформаційної безпеки підприємства в умовах неоіндустріального суспільства

Розвиток бізнесу перебуває у постійному русі і динамічно змінюється під впливом конкуренції та процесів глобалізації. Глобальний етап інтеграції економічних систем безпосередньо пов'язаний з багатоплановим процесом розширення та поглиблення світогосподарських зв'язків завдяки підвищенню мобільності факторів і результатів виробництва (макрорівень) та залучення фірми до міжнародних операцій (мікрорівень) [4, 32]. Проте, разом із швидкими темпами зростання економічних процесів при здійсненні господарської діяльності зростає і роль інформаційної безпеки підприємства.

При захисті інформації слід перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на усіх носіях, що маються на підприємстві. Загрози інформаційної безпеки поділяються на внутрішні та зовнішні. 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, 46].

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) недосконалість використовуваної системи захисту інформації; в) використання «піратського» програмного забезпечення; саботаж персоналу; г) низьку кваліфікацію співробітників; ґ) недостатню пожежну, технічну безпеку приміщень, будівель підприємства [2, 46].

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.

Для того, щоб система забезпечення інформаційної безпеки організації діяла вона повинна ґрунтуватися на наступних принципах [6]:

1) принцип комплексності, тобто при створенні систем захисту інформації повинна бути передбачена можливість виникнення всіх можливих загроз для конкретної організації. Вико-

ристовувані 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 цілодобовою;

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. Водночас вартість захисної системи не повинна перевищувати розмір можливого збитку і витрат на її обслуговування та функціонування.

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 буде 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).

Джерела та література

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, 2016. P. 270−271.
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. Луцьк: ПП Іванюк, 2013. 273 с.
6. Крюков О. І. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво.* 2007. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12

Олійник В. – студентка 4-го курсу

Науковий керівник: викл.
Л. Федоренко
Ніжинський агротехнічний коледж
м. Ніжин, Україна

Необхідність забезпечення фінансово-економічної безпеки підприємства

Фінансова безпека є невід'ємною складовою фінансового менеджменту підприємства та повинна бути реалізована в системі певних стратегічних і тактичних заходів та відповідати сучасним умовам господарювання.

Головною метою фінансово-економічної безпеки виступає гарантування фінансової стійкості та максимально ефективного функціонування підприємства у поточному періоді та висо-