УДК 658

Нагорняк І. С.
старший викладач кафедри економіки та фінансів
Тернопільський національний
Технічний університет імені Івана Пулюя
Нагорняк Г. С.
к.т.н., доцент кафедри менеджменту
інноваційної діяльності та підприємництва
Тернопільський національний
Технічний університет імені Івана Пулюя

ІНФОРМАЦІЙНА БЕЗПЕКА ПЕРСОНАЛУ У СИСТЕМІ СКЛАДОВИХ СОЦІАЛЬНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ МАШИНОБУДІВНИХ ПІДПРИЄМСТВ УКРАЇНИ: ОСНОВНІ ЗАГРОЗИ ТА ШЛЯХИ ЇХ НЕЙТРАЛІЗАЦІЇ

Актуальність проблеми захисту інформації сьогодні не викликає сумнівів. Успіх сучасного підприємства та його розвиток в умовах гострої конкуренції у значній мірі залежать від застосування інформаційних технологій, а, отже, від ступеня забезпечення інформаційної безпеки. Атаки на інформаційні та комунікаційні системи промислових підприємств України, у тому числі і машинобудування, відбуваються постійно. Ситуація ускладнюється також тим, що вся економіка і бізнес зокрема вже давно залежить від ІТ (системи електронної комерції, IP-телефонії, ERP-системи, електронної пошти тощо). Більшість українських підприємств постійно зазнають збитків, пов'язані з порушенням інформаційної безпеки персоналу, не здатні оцінити збиток або хоча б виявити багато з цих порушень. Збитки від порушень інформаційної безпеки персоналу можуть виражатися у витоку конфіденційної інформації, втрати робочого часу на відновлення даних, ліквідацію наслідків вірусних атак тощо. Метою забезпечення соціально-економічної безпеки підприємства є мінімізація загроз розвитку підприємства та забезпечення збереження та розвитку персоналу підприємства. У даному контексті актуальним питанням для машинобудівних підприємств на сьогодні є об'єкти загроз: персонал, матеріальні цінності, інформаційні ресурси та сама діяльність підприємства. Таким чином, безпека функціонування підприємства включає в себе й соціально-економічну безпеку. Відповідно, система забезпечення соціально-економічної безпеки підприємства повинна вирішувати наступні завдання:

- прогнозування й організація діяльності по попередженні можливих загроз соціально-економічній безпеці;
- виявлення, аналіз та оцінка виниклих реальних загроз соціально-економічній безпеці, а також прийняття управлінських рішень по їх нейтралізації;
- підбір достатнього рівня кваліфікації персоналу та оцінка ефективності його функціонування;
- захист інформаційного середовища, комерційної таємниці та досягнення високого рівня інформаційного забезпечення роботи;

– забезпечення безпеки персоналу, капіталу, майна та комерційних інтересів;
– недопущення проникнення на підприємство структур економічної розвідки конкурентів, організованої злочинності й окремих осіб з протиправними намірами;
– вироблення найбільш оптимальних управлінських рішень по питаннях стратегії й тактики соціально-економічної діяльності підприємства;
– організація системи контролю за ефективністю функціонування системи соціально-економічної безпеки, вдосконалення її елементів.

Управління інформаційною безпекою персоналу – це циклічний процес, що включає усвідомлення ступеня необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки персоналу на підприємстві; оцінку інформаційних ризиків; планування заходів по обробленні ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу по здійсненню захисних заходів; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії [3, 66].

Основними загрозами інформаційній безпеці персоналу у системі складових соціально-економічної безпеки в умовах функціонування підприємств машинобудування України, на наш погляд, є наступні: порушення режиму збереження комерційної таємниці; інформаційне шпигунство; вихід з ладу комп'ютерної техніки; відсутність ієрархічної системи доступу до інформації; наявність величезної кількості документації та відсутність інформаційних технологій в обліково-аналітичній роботі; відсутність корпоративної системи зв'язку між підрозділами й окремими працівниками підприємства; низька ділова репутація [1, 64].

Вважаємо, що важливими умовами забезпечення ефективності управління соціально-економічною безпекою функціонування машинобудівного підприємства є:
– інформаційна забезпеченість процесу управління;
– допустимі тривалість циклу управління і рівень перешкод у ньому;
– захищеність контуру управління від зовнішніх перешкод;
– здатність системи до виконання своїх функцій у всьому діапазоні зовнішніх умов, і більш широко – загальна надійність системи;
– допустима вартість системи, включаючи витрати на її створення і функціонування;
– спеціальні вимоги залежно від призначення системи [2, 136].

Для успішного управління соціально-економічною безпекою машинобудівного підприємства повинні бути забезпечені наступні підсистеми:
– підсистема планування та прогнозування, яка дозволятиме чітко визначити цілі управління;
– інформаційна підсистема (фінансовий и управлінський облік), яка у будь-який момент зможе забезпечити управління актуальною, повною та точною інформацією про стан керованого об'єкта та зовнішнього середовища, а також про тенденції їх зміни у майбутньому;
– аналітична підсистема, тобто мати у своєму розпорядженні спеціалістів, інструментарій та методи діагностики, за допомогою яких на основі інформації, що надходить, могли б зробити в обмежені терміни

обґрунтований висновок про необхідні управлінські впливи на об'єкт управління (розрахувати управлінські впливи);
- ефективна виконуюча підсистема (контроль), що дозволяє швидко та точно реалізувати управлінські впливи;
- підсистема зворотного зв'язку (прийняття управлінських рішень) для оцінювання результату керуючого впливу на стан об'єкта управління та внесення змін у випадку отримання відхилення досягнутого стану системи від бажаного стану за межі заданого інтервалу – інтервалу допустимих відхилень [4, 177].

До істотних прогалин інформаційної безпеки підприємства варто віднести недостатньо вивчені аспекти дослідження інформаційної безпеки персоналу, визначення соціально-економічної суті цього феномену. Під інформаційною небезпекою розуміється використання об'єктивних і суб'єктивних інформаційних факторів, що володіють негативною дією для нанесення шкоди кому-небудь безпосередньо або опосередковано в інформаційній сфері. У даному випадку мається на увазі небезпека, що породжується самим процесом інформатизації та інформаційними впливами. У результаті нейтралізації забезпечується надійний та всебічний захист названих суб'єктів від особливого виду небезпек, основою яких є негативний вплив різних видів інформації, в основному, духовного, соціального й економічного характеру. Загрози, що існують у вигляді інформаційних потоків і каналів, здатні виникати та виявлятися як громадські вибухи, потрясіння, хвилювання, кризи тощо [5, 49].

Виходячи з аналізу інформаційних загроз, можна констатувати, що інформаційна безпека персоналу у системі складових соціально-економічної безпеки машинобудівного підприємства – це такий стан інформаційної сфери, при якому забезпечені надійний і всебічний захист персоналу машинобудівного підприємства шляхом подолання або нейтралізації особливого виду загроз, які виступають у формі організованих або стихійно виникаючих інформаційних каналів і потоків. Керівник зобов'язаний контролювати ситуацію в своїй організації, підрозділі, проект і у взаєминах із замовниками. Це означає бути обізнаним про те, що відбувається, своєчасно дізнаватися про всі позаштатних ситуаціях і уявляти собі, що насамперед треба буде зробити, в тому чи іншому випадку. В організації існує кілька рівнів управління, починаючи з менеджерів вищої ланки і закінчуючи конкретним виконавцями, і на кожному рівні ситуація повинна залишатися під контролем.

ЛІТЕРАТУРА:

1. Беседин А.Л. Экономическая безопасность предприятия в контексте системного подхода к решению проблемы защиты конфиденциальной информации / А.Л. Беседин, В.В. Беляев // Финансы и кредит. – 2004. – № 27. – С. 63-68.
2. Бондаренко С. С. Машинобудівні підприємства: потреба в нових управлінських інструментах / С. С. Бондаренко // Економіка. Менеджмент. Підприємництво. Зб. наук. праць Східноукраїнського національного університету імені Володимира Даля. Вип. 21. Ч. ІІ. – С. 135-140.
3. Живко З.Б. Аналіз та оцінка системи мотивації персоналу як чинника безпеки / З.Б. Живко // Актуальні проблеми економіки. – 2009, № 10 (100). – С. 65-73.

4. Живко З.Б. Комплексный подход к управлению безопасностью предприятия: взаимодействие подсистем и роль менеджера [Текст] / З.Б. Живко // Научный диалог. – 2013. – №1 (13): История. Социология. Экономика. – С. 177-187.
5. Одинцов А. А. Экономическая и информационная безопасность предпринимательства / А.А. Одинцов. – М.: Академия, 2006. – 336 с.

Падалка А. М.
к.ю.н., в.о. завідувача кафедри фінансових розслідувань
факультету підготовки, перепідготовки та підвищення
кваліфікації працівників податкової міліції
Університет державної фіскальної служби України

РОЗСЛІДУВАННЯ ОРГАНІЗОВАНОЇ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ У СФЕРІ ОПОДАТКУВАННЯ, ЗДІЙСНЮВАНОЇ З ВИКОРИСТАННЯМ СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

1. Ефективність розслідування організованої злочинної діяльності у сфері оподаткуваання ще залишається досить низькою. Це зумовлено: складним процесом доказування таких кримінальних правопорушень, потужною протидією розслідуванню з боку учасників організованих злочинних угруповань, проблемами з організацією використанням криміналістичних комплексів, недоліками професійної підготовки слідчих та певною мірою незнанням ними особливостей використання спеціальних знань в ході розслідування зазначеної організованої злочинної діяльності, особливо здійснюваної з використанням сучасних комп'ютерних технологій.

2. Як свідчать здійснені нами узагальнення, поширеними формами використання спеціальних знань, під час розслідування організованої злочинної діяльність у сфері оподаткування, здійснюваної з використанням комп'ютерних технологій є: а) призначення судово-економічної експертизи та комп'ютерно-технічних експертиз; б) звернення слідчого за письмовою консультацією до відповідного спеціаліста; в) залучення спеціаліста до участі у слідчих (розшукових) діях; г) призначення документальних перевірок на вимогу слідчого; ґ) проведення ревізій; д) безпосереднє використання спеціальних знань самим слідчим, під час проведення слідчих (розшукових) дій.

3. Розслідування організованої злочинної діяльності у сфері оподаткування, здійснюваної з використанням сучасних комп'ютерної техніки не можливе без проведення комп'ютерно-технічної експертизи. Серед проблем, які виникають у слідчих, під час призначення такої експертизи слід відмітити: 1) зумовлені недостатнім фінансуванням виконання даних експертиз на договірній основі; 2) зумовлені недостатньою кількістю і підвищеною завантаженістю експертів; 3) зумовлені визначенням завдань експертизи та формулюванням питань експерту; 4) зумовлені визначенням переліку об'єктів, які доцільно направляти на експертизу; 5) зумовлені відсутністю відповідної експертної методики для вирішення тих чи інших питань, що поставлені перед експертом.