них знать, отриманих навичок, накопиченого досвіду та особистими характеристиками працівника залежно від організаційно технічних умов.

Трудовий потенціал підприємства є сумою частин, що її складає кожен окремо взятий працівник. Об'єднання окремо взятих робітників в єдину систему націлені на виконання певної роботи або процесу створюють колективну працю. При формуванні конкурентоспроможного трудового потенціалу необхідно враховувати особливості формування та традиції колективу, взаємовідносини між робітниками. Крім індивідуальних характеристик необхідно звернути увагу на розташування підприємства, його розміри, специфіку виробництва, статевовікові показники тощо.

Тож, трудовий потенціал вимагає постійного моніторингу та реагування на зміни що відбуваються як ззовні, так і в середині підприємства. Ефективна реалізація трудового потенціалу гарантує міцні позиції на ринку та стабільність при жорсткій конкуренції. Постановка цілі розвитку трудового потенціалу дає впевненість у взаємозамінності робітників у разі виникнення непередбачуваних ситуацій та підготовки планової зміни кадрів у довготривалій перспективі.

В даний час серед дослідників існує кілька підходів до трактування наукового поняття «трудовий потенціал», основними з яких є: ототожнення даної категорії з поняттями «робоча сила» або «трудові ресурси», уявлення про трудовий потенціал як про форму особистого або людського фактора, облік впливу на трудовий потенціал економічних відносин або ускладнюються форм суспільного життя. Порівняльна характеристика категорій в області економіки праці та управління персоналом допомогла визначити серед них місце категорії «трудовий потенціал», виявити сутність поняття «трудовий потенціал», яке представляє собою ступінь можливої участі працівників у трудовій діяльності з урахуванням їх психофізіологічних, соціально-демографічних, кваліфікаційних та особистісних особливостей, а також можливостей їх розвитку в процесі праці. Основою трудового потенціалу окремого працівника є людський потенціал, як сукупність можливостей, що реалізуються людиною в процесі праці. Реалізований трудовий потенціал (в сукупності його складових), в свою чергу, входить до складу категорії «людський капітал» [2].

Джерела та література

1. Веснин В. Р. Основы менеджмента: учеб. пособие. Москва: Элит-2000. 440 с.
2. Поташин Я. С. Трудовой потенциал персонала управления организации. URL: http://www.rusnauka.com/8._NPE_2007/Economics/19166.doc.htm (дата звернення: 08.10.2020).
3. Судакова Е. С. Взаимосвязь развития трудового потенциала персонала и эффективности организации. *Интернет-журнал «Науковедение»*. 2014. № 3 (22). URL: http://naukovedenie.ru/PDF/159EVN314.pdf (дата звернення: 08.10.2020).

Нестеров О. − к. т. н., доц.;
Перепечаєв С. − к. д. п., ст. викл.
Азовський морський інститут
Одеської національної морської
академії, м. Маріуполь, Україна

Проблеми навігаційної безпеки в умовах індустріального суспільства

Трагедії на морі, пов'язані з навігаційної безпекою суден, траплялися на всьому протязі людського існування. Однак, загибель лайнера «Титанік» 14 квітня 1912 р., яка забрала життя 1,5 тисячі людей потрясла людство. Ця подія змусила громадськість спробувати протиставити морським трагедій свої знання і організованість. Тому, 1912 по суті, був початком сучасної епохи боротьби за безпеку плавання суден.

У 1914 р. приймається Міжнародна конвенція з охорони людського життя на морі СОЛАС-14. Цей документ всім своїм змістом висловлював турботу про людині-зобов'язував збільшити кількість рятувальних засобів, уточнював конструктивні особливості судна, що не допускають швидкого затоплення приміщень судна. Подальші уточнення і доповнення даної конвенції відбилися в появі СОЛАС-29, СОЛАС-48, СОЛАС-60, СОЛАС-74. Згодом збільшувалася кількість держав, які ратифікували цей документ, паралельно цьому збільшився і обсяг самого документа. Здавалося б, все питання охорони людського життя на морі позначені. Світова громадськість погодилася з ними і почала активно впроваджувати запропоновані в конвенції заходи. Але ситуація активно не змінювалася і, на сьогоднішній день за даними деяких джерел в морських катастрофах гине в середньому 300 суден. В 1993 році розробляється і на 18-й Асамблеї ІМО резолюція А.741 (18) приймається Міжнародний кодекс з управління безпечною експлуатацією суден і запобігання забруднень (ISM CODE) або МКУБ.

Метою цього документа є створення стандарту системи, що забезпечує безпечне плавання суден. Стандарт системи повинен не тільки забезпечити безпечне плавання, але і полегшити завдання контролю готовності судна до виходу в море. Далі в 1995 р. розробляється і резолюція А.787 (19), приймаються організаціоннние принципи системи контролю суден. Це резолюція носить назву «Процедури контролю суден державою порту».Тепер здавалося б, зроблено все для зменшення аварійності, проте число аварійних пригод не зменшується. Тобто мета, до якої всі ці роки прагнуло ІМО досягнута. Тому світова морська громадськість, включаючи Міжнародну морську організацію (ІМО), берегову охорону розвинених морських держав, асоціації фрахтувальників, судновласників, класифікаційних суспільств і передових судноплавних компаній направляють всезростаючі зусилля на контроль над «людським чинником» для забезпечення безпеки мореплавання на морському флоті. Досягнення сучасної науки дозволили використати для цих цілей системний підхід. Хотілося б звернути увагу на основні причини, які не дозволяють досягти бажаного результату і перш за все це так званий «людський фактор», про який в останні роки йде велика полеміка. На цей рахунок навіть існує резолюція ІМО А.884 (21) «Керівництво по розслідування людського фактора в морських аваріях та інциденти».

Мабуть, якщо уточнити, то в самому «людський фактор» мова повинна йти про професіоналізм насамперед так як все в цьому світі пов'язане з людиною. Отже, морська інспекція повинна звернути найсерйознішу увагу не тільки на готовність судна зустріти достойно аварійну ситуацію, а й вжити відповідних заходів на березі, щоб не допускати навігаційної аварії. На жаль, ми забули, що вже давно не є володарями потужного флоту і що головне сьогодні наше надбання і наш джерело аварійності це порти і прибережна зона плавання. Більшість аварій трапляються в обмежених водах, поблизу підходів до портів, де щільний рух суден. Якраз в цих місцях і в цей час, екіпаж найбільш завантажений. Він повинен ефективно використовувати всі наявні технічні та людські резерви, а також функції колективу для безпечного управління судном. Цікава статистика сьогоднішнього дня по розподілу винних за аварію:

1) судноводії – 25 %;
2) лоцмани – 5 %;
3) механіки − 2 %;
4) поломка устаткування – 8 %;
5) рядовий склад – 17 %;
6) механічні несправності – 15 %;
7) береговий склад − 14 %;
8) інші − 14 %.

Сьогодні Україна є однією з провідних країн по підготовці плавскладу для світового флоту, тому і від нас залежить вирішення проблем навігаційної безпеки. У зв'язку з цим навчальним закладам перш за все необхідно приділити увагу такому питанню, як отримання курсантами плавального цензу, необхідного для оформлення робочого диплома. Цього можна досягти шляхом укладення договорів з власниками судноплавних компаній, оскільки нашого флоту недостатньо. Якщо керівники галузі підійдуть до вирішення цього питання з серйозними намірами, наша країна залишиться в статусі морської держави.

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-