УДК 331.1:368.03

КАДРОВА БЕЗПЕКА В СИСТЕМІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ СТРАХОВИХ КОМПАНІЙ

© 2015 **ЖАБИНЕЦЬ О. Й.**

УДК 331.1:368.03

Жабинець О. Й. Кадрова безпека в системі фінансово-економічної безпеки страхових компаній

У статті досліджена кадрова безпека в системі фінансово-економічної безпеки страхових компаній, визначено її вплив на формування інформаційної та фінансової безпеки страховика, проаналізовано основні етапи забезпечення інформаційної безпеки через безпеку персоналу в міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013. Автор вважає, що інтенсивні зміни сучасного глобального інформаційного простору ставлять нові вимоги до підбору, навчання та звільнення персоналу, а кадрова безпека сьогодні є визначальною в системі фінансово-економічної безпеки будь-якого суб'єкта господарювання, у т. ч. страхової компанії. Прийняття персоналом різних рівнів ефективних рішень у фінансово-господарській діяльності страховика є запорукою його фінансової стабільності, а відтак – фінансової безпеки, а можливість протидіяти витокам конфіденційної інформації та даних, що складають комерційну таємницю, через персонал страховика складає основу його інформаційної безпеки. Доведено, що в міжнародній практиці вирішенню проблем кадрової безпеки приділяється значна увага, зокрема, у міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013 чітко прослідковується зв'язок між безпекою персоналу та інформаційною безпекою організації, починаючи з прийняття працівника на роботу та закінчуючи розірванням трудового договору.

Ключові слова: *кадрова безпека страховика, фінансово-економічна безпека страхових компаній, інформаційна безпека, міжнародний стандарт інформаційної безпеки ISO/IEC 27002:2013.*

Рис.: *2.* ***Бібл.:*** *10.*

Жабинець Ольга Йосифівна *– кандидат економічних наук, доцент, доцент кафедри фінансів, Львівський державний університет внутрішніх справ (вул. Городоцька, 26, Львів, 79066, Україна)*

E-mail: *olza@ukr.net*

УДК 331.1:368.03

Жабинец О. И. Кадровая безопасность в системе финансово-экономической безопасности страховых компаний

В статье исследована кадровая безопасность в системе финансово-экономической безопасности страховых компаний, определено ее влияние на формирование информационной и финансовой безопасности страховщика, проанализированы основные этапы обеспечения информационной безопасности через безопасность персонала в международном стандарте информационной безопасности ISO / IEC 27002: 2013. Автор считает, что интенсивные изменения современного глобального информационного пространства выдвигают новые требования к подбору, обучению и увольнению персонала, а кадровая безопасность сегодня является определяющей в системе финансово-экономической безопасности любого предприятия, в т. ч. страховой компании. Принятие персоналом различных уровней эффективных решений в финансово-хозяйственной деятельности страховщика является залогом его финансовой стабильности и как следствие – финансовой безопасности, а возможность противодействовать утечкам конфиденциальной информации и данных, составляющих коммерческую тайну, через персонал страховщика составляет основу его информационной безопасности. Доказано, что в международной практике решению проблем кадровой безопасности уделяется значительное внимание, в частности, в международном стандарте информационной безопасности ISO / IEC 27002:2013 четко прослеживается связь между безопасностью персонала и информационной безопасностью организации, начиная с приема работника на работу и заканчивая расторжением трудового договора.

Ключевые слова: *кадровая безопасность страховщика, финансово-экономическая безопасность страховых компаний, информационная безопасность, международный стандарт информационной безопасности ISO / IEC 27002:2013.*

Рис.: *2.* ***Бібл.:*** *10.*

Жабинец Ольга Иосифовна *– кандидат экономических наук, доцент, доцент кафедры финансов, Львовский государственный университет внутренних дел (ул. Городоцкая, 26, Львов, 79066, Украина)*

E-mail: *olza@ukr.net*

UDC 331.1:368.03

Zhabynets O. Yo. Personnel Security in the System of Financial-Economic Security of Insurance Companies

In the article the personnel security in the system of financial-economic security of insurance companies has been researched, its influence on establishing the information and financial security of insurer has been determined, the main stages of implementation of information security by means of the personnel security in the international standard for information security ISO/IEC 27002: 2013 has been analyzed. The author believes that intense changes of modern global information space put forward new requirements for selection, training and termination of staff, because nowadays personnel security is decisive in the system of economic-financial security of any company, including insurance companies. Acceptance by the staff of various levels of effective solutions in the financial-economic activity of insurer is pivotal for its financial stability and, as a consequence, its financial security together with ability to counter leakages of confidential information and data, which comprise commercial secret, so that assistance of the staff becomes the core of the insurer's information security. It has been proven that in international practice solving the problems of personnel security has received considerable attention, inter alia, in the international information security standard ISO / IEC 27002:2013 clear relationship between personnel security and information security of organization, from the hiring of an employee and to the termination of the employment contract, is well discernible.

Key words: *personnel security of insurer, financial-economic security of insurance companies, information security, international standard for information security ISO/IEC 27002:2013.*

Pic.: *2.* ***Bibl.:*** *10.*

Zhabynets Olga Yo. *– Candidate of Sciences (Economics), Associate Professor, Associate Professor of the Department of Finance, Lviv State University of Internal Affairs (vul. Gorodotska, 26, Lviv, 79066, Ukraine)*

E-mail: *olza@ukr.net*

Інтенсивні зміни сучасного глобального інформаційного простору ставлять нові вимоги до організації системи кадрової безпеки на підприємствах різних сфер національної економіки. Не є винятком і вітчизняна сфера страхування, яка постійно потребує висококваліфікованих менеджерів, андеррайтерів, агентів, аварійних комісарів, актуаріїв та інших спеціалістів, що виступають запорукою ефективності функціонування бізнесу, його прибутковості та конкурентоспроможності. З огляду на це, дослідження питань забезпечен-

ня кадрової безпеки страховиків як важливої складової системи їх фінансово-економічної безпеки, набирає сьогодні особливої актуальності.

Проблеми забезпечення кадрової безпеки розглядаються у працях багатьох вітчизняних і зарубіжних науковців, серед яких Живко З. Б., Кравченко В. О., Мехеда Н. Г., Томаневич Л. М., Чаплигіна Ю. С., Чередниченко Н. В., Чумарін І. Г. та багато інших. Водночас у сучасній науковій літературі практично відсутні дослідження, що пов'язані з безпекою персоналу страхових компаній, а також із встановленням взаємозв'язків кадрової безпеки з інформаційною та фінансовою безпекою страховиків, що і обумовило вибір тематики даної наукової статті.

Метою статті є дослідження місця кадрової безпеки в системі фінансово-економічної безпеки страхових компаній та визначення її впливу на формування інформаційної безпеки страховика.

Різні науковці, аналізуючи складові економічної безпеки підприємства, поряд з іншими виділяють: кадрову [1; 2; 3], інтелектуально-кадрову [4], кадрову та інтелектуальну [5; 6] або інтелектуальну [7] складові. Оскільки інтелектуальним потенціалом володіє виключно людина як суб'єкт та об'єкт кадрової безпеки, а також тому, що інтелектуальний потенціал є вторинним по відношенню до кадрів, виступаючи одним з елементів кадрової безпеки, то, на нашу думку, варто вживати термін «кадрова безпека («безпека персоналу») або «інтелектуально-кадрова безпека».

Під загальним терміном «кадрова безпека» («безпека персоналу»), з яким ми погоджуємось, більшість науковців розуміє процес запобігання негативним впливам на економічну безпеку підприємства за рахунок ризиків і загроз, пов'язаних із персоналом, його інтелектуальним потенціалом і трудовими відносинами в цілому.

Про важливість кадрової безпеки в системі економічної безпеки будь-якого господарюючого суб'єкта говорить статистика. Так, близько 80% збитку матеріальним активам компаній наноситься їх власним персоналом. Тільки 20% спроб злому мереж і отримання несанкціонованого доступу до комп'ютерної інформації приходить ззовні, інші 80% випадків – спровоковані за участю персоналу [8].

Кадрова безпека, на нашу думку, є визначальною в системі фінансово-економічної безпеки будь-якого суб'єкта господарювання, у т. ч. страхової компанії. Від неї напряму залежить рівень забезпеченості усіх інших складових безпеки, зокрема фінансової та інформаційної безпеки (*рис. 1*).

Так, прийняття персоналом різних рівнів ефективних рішень у фінансово-господарській діяльності страховика є запорукою його фінансової стабільності, а відтак – фінансової безпеки. З іншого боку, – можливість протидіяти витокам конфіденційної інформації та даних, що складають комерційну таємницю, через персонал страховика складає основу інформаційної безпеки.

Недарма в міжнародній практиці вирішенню проблем кадрової безпеки приділяється значна увага. Так, у міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013 чітко прослідковується зв'язок між безпекою персоналу та інформаційною безпекою організації, починаючи з прийняття працівника на роботу та закінчуючи розірванням трудового договору (*рис. 2*).

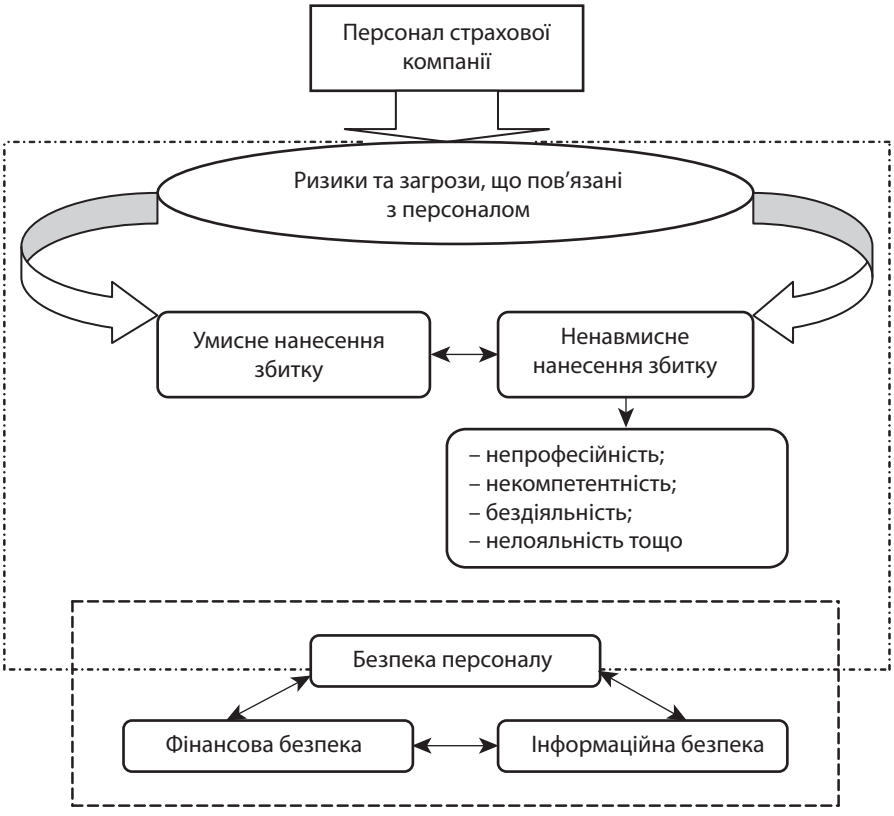

Рис. 1. Безпека персоналу та її взаємозв'язок із фінансовою та інформаційною безпекою страховика

Джерело: розроблено автором.

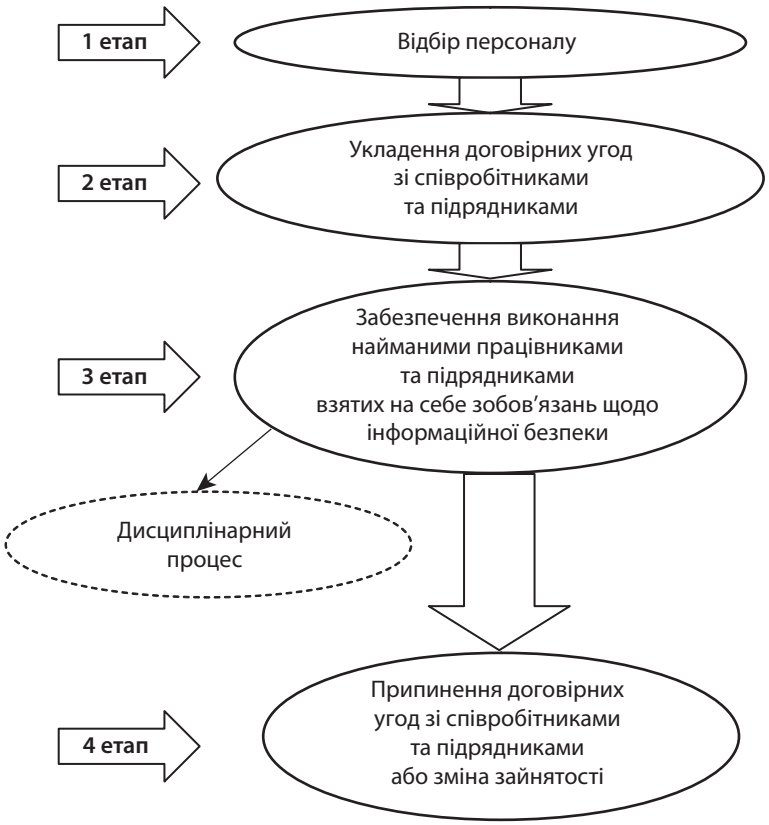

Рис. 2. Основні етапи забезпечення інформаційної безпеки через безпеку персоналу в міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013

Джерело: побудовано автором за [9].

На етапі відбору персоналу (*1 етап*) стандартом інформаційної безпеки ISO/IEC 27002:2013 вимагається проведення верифікаційних перевірок усіх кандидатів на посади. Ці перевірки необхідно здійснювати у відповідності до законодавства, правил та етики, враховуючи потреби бізнесу, класифікацію інформації, яка буде доступна для перегляду, і можливі ризики.

Перевірка повинна включати таке:

1) наявність задовільних рекомендацій, наприклад, одна ділова та одна особиста;

2) перевірка (на повноту і точність) анкетних даних кандидата;

3) підтвердження заявлених академічних та професійних кваліфікацій;

4) незалежна перевірка особистих даних (паспорта чи аналогічного документу);

5) більш детальні перевірки, такі як перевірка репутації або судимостей [9].

Водночас, якщо робота за першопочатковим призначенням або внаслідок просування по службі вимагає від особи мати доступ до засобів обробки інформації і, зокрема, обробки конфіденційної інформації, наприклад, фінансової або інформації вищої категорії конфіденційності, організація повинна провести більш детальні перевірки кандидатів.

Процес відбору також повинен виконуватись підрядниками. У такому випадку в угоді між організацією і підрядником необхідно чітко вказати обов'язки підрядника з проведення відбору і процедури повідомлення, яких необхідно дотримуватись, якщо відбір не був завершеним, або якщо результати дають привід для сумнівів або занепокоєння.

Інформація про всіх кандидатів, які розглядаються на посади, повинна бути зібрана та оброблена відповідно до законодавства. У свою чергу, кандидати повинні бути завчасно проінформовані про заходи щодо відбору.

На *другому етапі* (див. рис. 2) передбачається укладення договірних угод зі співробітниками та підрядниками, які мають містити їх обов'язки та обов'язки організації щодо інформаційної безпеки. Договірні зобов'язання для співробітників або підрядників повинні відображати політику інформаційної безпеки організації, а тому всі співробітники та підрядники, які отримали доступ до конфіденційної інформації, мають підписати угоду щодо конфіденційності або нерозголошення перед тим, як вони отримають доступ до засобів обробки інформації.

Крім того, договірні зобов'язання повинні передбачати:

1) законні обов'язки та права працівника або підрядника, наприклад, ті, що стосуються законів щодо авторських прав або законодавства про захист даних;

2) відповідальність за класифікацію інформації та управління активами організації, пов'язаних з інформацією, засобами обробки інформації та інформаційних послуг, до яких має відношення працівник або підрядник;

3) обов'язки працівника або підрядника щодо обробки інформації, отриманої від інших компаній або зовнішніх сторін;

4) заходи, які повинні вживатися, якщо працівник чи підрядник ігнорує вимоги безпеки організації.

Завдання інформаційної безпеки та відповідальність повинні бути доведені до кандидатів протягом процесу найму на роботу. У разі необхідності відповідальність, що міститься в умовах трудового договору (контракту), можна продовжити на певний період часу після його закінчення та звільнення з роботи.

Обов'язки працівників та підрядників щодо захисту конфіденційності, захисту даних, етики, належного використання обладнання та коштів організації тощо можна систематизувати в кодекс поведінки організації.

На *третьому етапі*, напевно найскладнішому, необхідно забезпечити виконання найманими працівниками та підрядниками взятих на себе зобов'язань щодо інформаційної безпеки під час здійснення покладеної на них роботи. На цьому етапі ключова роль відводиться керівництву фірми та його професійності.

Завдання управлінського персоналу щодо дотримання працівниками та підрядниками зобов'язань з інформаційної безпеки (відповідно до міжнародного стандарту інформаційної безпеки ISO/IEC 27002:2013) є такими:

- здійснення належної поінформованості працівників та підрядників щодо обов'язків з інформаційної безпеки перед тим, як вони отримають доступ до конфіденційної інформації або інформаційних систем;
- забезпечення вказівками працівників та підрядників щодо очікувань у сфері захисту інформації в залежності від їх ролі в організації;
- мотивація працівників та підрядників щодо виконання політики інформаційної безпеки;
- досягнення належного рівня знань працівниками та підрядниками з інформаційної безпеки відповідно до функцій та посадових обов'язків в організації;
- забезпечення відповідності умовам роботи, які містять політику інформаційної безпеки організації та відповідні методи роботи;
- можливість підтримання працівниками та підрядниками відповідних навичок і кваліфікації, а також їх регулярне навчання;
- забезпечення анонімним каналом для повідомлення про порушення політики або процедур інформаційної безпеки («свисток дме») [9].

Керівництво має демонструвати свою підтримку політики, процедур і механізмів контролю інформаційної безпеки, а також діяти як рольова модель. Адже якщо співробітники і підрядники будуть неналежно проінформовані щодо своїх обов'язків із забезпечення інформаційної безпеки, вони можуть бути причиною значних збитків організації. І навпаки – мотивований персонал, ймовірно, буде більш надійним, внаслідок чого виникатиме менше інцидентів інформаційної безпеки.

Одним з важливих елементів кадрової безпеки компанії вважається такий аспект діяльності служби персоналу, як організація навчання співробітників. Адже фахівці з безпеки не можуть проконтролювати та попередити всі ризики, що можуть завдати втрат компанії, тому допомога персоналу є вкрай необхідною.

Крім стандартно запланованих заходів, таких як підвищення професійної кваліфікації, перенавчання і т. п., у планах і програмах служби персоналу та служби безпеки значне місце має займати додаткове інформування фахівців різних підрозділів з питань безпеки. Побудова системи економічної безпеки підприємства не буде вважатися завершеною, якщо в ній не передбачено спрямування навчання та підвищення кваліфікації саме з безпеки. Причому не тільки співробітників профільного підрозділу, але і всіх інших працівників. Як правило, штатних фахівців відділу безпеки та охорони відправляють на відповідні семінари і курси, а про решту персоналу забувають [10].

Внутріфірмове навчання у сфері безпеки, як правило, організовується за такими основними напрямами:

1) навчання колективним та індивідуальним діям в екстрених ситуаціях;

2) навчання методам захисту інформації та інтелектуальної власності;

3) навчання способам виявлення і запобігання неправомірних дій інших працівників;

4) навчання загальним і спеціальним методам розпізнавання шахрайських дій з боку клієнтів, постачальників та інших суб'єктів ринку;

5) навчання правилам особистої (побутової) безпеки;

6) навчання правилам техніки виробничої безпеки [10].

Якісна організація навчання за зазначеними вище напрямами повинна включати в себе не тільки доведення інформації до персоналу в той або інший спосіб, але й перевірку відповідних знань у вигляді заліків та практичних тренувань, а питання з тематики занять повинні включатися в опитувальні листи при атестації. Проходження навчання за найбільш важливим темами повинно документуватися в спеціальних журналах (іноді з видачею внутрішньофірмових сертифікатів і дипломів), що також є одним з факторів мотивації, оскільки навчання все ж таки безкоштовне. Щоб ефект від занять був довгостроковим, посадові чи процедурні інструкції, технологічні процеси повинні повторювати правила і вимоги, озвучені на заняттях і курсах.

Вимоги стандарту інформаційної безпеки ISO/IEC 27002:2013 у даному аспекті передбачають зокрема розробку Програми ознайомлення з інформаційною безпекою, яка повинна доводитись до відома працівників та підрядників у формі тренінгів через навчання в класі, дистанційне навчання, Інтернет (веб-сайти), самостійно або іншим чином. Крім того, Програма повинна передбачати низку інформаційно-просвітницьких заходів, таких як, наприклад, «День інформаційної безпеки», а також випуск буклетів або інформаційних бюлетенів.

Освіта з інформаційної безпеки та тренінги мають також охоплювати такі загальні аспекти, як:

а) заявлена прихильність керівництва щодо інформаційної безпеки в межах всієї організації;

б) необхідність ознайомлення та дотримання правил безпеки інформації та зобов'язань, що відповідає політиці, стандартам, законам, постановам, договорам і угодам;

в) особиста відповідальність за свої власні дії та бездіяльність і загальна відповідальність щодо забезпечення захисту інформації, що належить організації та зовнішнім сторонам;

г) основні процедури інформаційної безпеки (наприклад, звітність по інцидентах інформаційної безпеки) та базові елементи управління (наприклад, пароль безпеки, контроль шкідливих програм і чисті екрани);

д) контактні пункти та ресурси для отримання додаткової інформації та консультацій з питань інформаційної безпеки, у тому числі подальша освіта з інформаційної безпеки і навчальні матеріали.

Ознайомлення з інформаційною безпекою і навчання повинні відбуватись періодично. Початкові знання та тренінги слід проводити для тих, хто переходить на нові посади з іншими вимогами щодо інформаційної безпеки, а не тільки для нових працівників, причому – до вступу на посаду. Важливо, щоб співробітники розуміли мету інформаційної безпеки та потенційний вплив, позитивний і негативний, їх власної поведінки. Обізнаність, освіта і навчання з інформаційної безпеки можуть проводитися окремо або разом з іншими навчальними заходами, наприклад, загальними IT-тренінгами або загальною підготовкою в галузі безпеки. Обізнаність, освіта і підготовка кадрів повинні відповідати кожному індивідуально, враховуючи вимоги посади, обов'язків і навичок.

Важливе значення на третьому етапі забезпечення інформаційної безпеки через безпеку персоналу в міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013 відводиться дисциплінарному процесу (див. рис. 2), який буде застосовуватись до співробітників – порушників інформаційної безпеки.

Офіційний дисциплінарний процес повинен забезпечити коректний і справедливий розгляд справ співробітників, які підозрюються у вчиненні порушення інформаційної безпеки, а також має передбачати шкалу оцінювання рівня кожного порушення, зокрема, аналіз таких факторів, як характер і ступінь тяжкості порушення, його вплив на бізнес, чи це перше або повторне порушення, чи був порушник належним чином підготовлений тощо. При цьому слід враховувати відповідне законодавство, господарські договори та інші фактори (за потребою).

Дисциплінарний процес повинен використовуватися і як стримуючий фактор для запобігання порушення співробітниками політики інформаційної безпеки, і як їх мотивація (стимул) до підтримання належного рівня інформаційної безпеки.

На *четвертому етапі* – припинення або зміни зайнятості – необхідно забезпечити захист інтересів організації при звільненні співробітників або зміні їх посадових обов'язків. З огляду на це, відповідальність та обов'язки з інформаційної безпеки, які необхідно виконувати протягом визначеного періоду після припинення трудових відносин, повинні міститися в контракті або угодах зі співробітниками та підрядниками (у т. ч. в угоді про конфіденційність, умовах роботи), що укладаються на початку співпраці між ними та організацією.

Відділ кадрів, як правило, несе відповідальність за весь процес припинення роботи і працює разом із керівником тієї особи, яка йде з посади, або підрядником з метою управління усіма аспектами забезпечення інформаційної безпеки.

ВИСНОВКИ

Інформатизація усіх сфер національної економіки вимагає застосування нових підходів до підбору, навчання та звільнення персоналу, а кадрова безпека є сьогодні визначальною в системі фінансово-економічної безпеки будь-якого суб'єкта господарювання, у т.ч. страхової компанії. Прийняття персоналом різних рівнів ефективних рішень у фінансово-господарській діяльності страховика є запорукою його фінансової стабільності, а відтак – фінансової безпеки, а можливість протидіяти витокам конфіденційної інформації та даних, що складають комерційну таємницю, через персонал страховика складає основу його інформаційної безпеки. З огляду на це вирішенню проблем кадрової безпеки в міжнародній практиці приділяється значна увага, зокрема, у міжнародному стандарті інформаційної безпеки ISO/IEC 27002:2013 чітко прослідковується зв'язок між безпекою персоналу та інформаційною безпекою організації, починаючи з прийняття працівника на роботу та закінчуючи припиненням трудового договору. ■

ЛІТЕРАТУРА

1. Чередниченко Н. В. Кадрова безпека як складова частина економічної безпеки підприємства / Н. В. Чередниченко // Управління фінансово-економічною безпекою : матеріали науково-практичної конференції, 28 серпня 2009 р. – Суми : СумДУ, 2009. – С. 51 – 53 [Електронний ресурс]. – Режим доступу : http://essuir.sumdu.edu.ua/handle/123456789/8570

2. Томаневич Л. М. Кадрова безпека підприємства як об'єкт теоретичного дослідження / Л. М. Томаневич // Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. – Львів: ЛьвДУВС, 2009. – Вип. 1. – С. 185 – 192.

3. Кравченко В. О. Кадрова безпека – основа економічної безпеки підприємства / В. О. Кравченко // Соціально-трудові відносини: теорія та практика : зб. наук. праць. – К. : КНЕУ, 2014. – № 1 (7). – С. 301 – 306.

4. Поскрипко Ю. А. Механізми вдосконалення інтелектуально-кадрової складової економічної безпеки підприємств / Ю. А. Поскрипко // Наукові записки УНДІЗ. – 2012. – № 2(22). – С. 118 – 120.

5. Штамбург Н. В. Складові економічної безпеки підприємства / Н. В. Штамбург // Бюлетень Міжнародного Нобелівського економічного форуму. – 2011. – № 1(4). – С. 490 – 496.

6. Мехеда Н. Г. Соціально-мотиваційні складові кадрової безпеки / Н. Г. Мехеда, А. І. Маренич // Фінансовий простір: міжнародний науково-практичний журнал / Черкаський інститут банківської справи Університету банківської справи НБУ (м. Київ). –Черкаси, 2012. – № 2 (6). – С. 44 – 51.

7. Волощук Л. О. Інтелектуальна складова економічної безпеки підприємства / Л. О. Волощук, Ю. А. Некіпелова // [Електронний ресурс]. – Режим доступу : http://economics.opu.ua/files/science/2014/ipredV_2014/43.pdf

8. Чумарин И. Г. Что такое кадровая безопасность компании / И. Г. Чумарин // Кадры предприятия. – 2003. – № 2 [Электронный ресурс]. – Режим доступа : http://www.kapr.ru/articles/2003/2/519.html

9. International standard ISO/IEC 27002. – Second edition. – Switzerland, 2013. – 80 p.

10. Чумарин И. Г. Укрепление безопасности компании через обучение сотрудников / И. Г. Чумарин // Кадры предприятия. – 2004. – № 10. – С/ 51 – 55 [Электронный ресурс]. – Режим доступа : http://www.kapr.ru/articles/2004/10/3558.html

REFERENCES

Cherednychenko, N. V. "Kadrova bezpeka iak skladova chastyna ekonomichnoi bezpeky pidpryiemstva" [Personnel security as part of economic security]. http://essuir.sumdu.edu.ua/handle/123456789/8570

Chumarin, I. G. "Chto takoe kadrovaya bezopasnost" [What is the safety of personnel]. http://www.kapr.ru/articles/2003/2/519.html

Chumarin, I. G. "Ukreplenie bezopasnosti kompanii cherez obuchenie sotrudnikov" [Strengthening the security of the company through staff training]. http://www.kapr.ru/articles/2004/10/3558.html

International standard ISO/IEC 27002. Switzerland, 2013.

Kravchenko, V. O. "Kadrova bezpeka – osnova ekonomichnoi bezpeky pidpryiemstva" [Personnel Security – the foundation of economic security]. *Sotsialno-trudovi vidnosyny: teoriia ta praktyka*, no. 1 (7) (2014): 301-306.

Mekheda, N. H., and Marenych, A. I. "Sotsialno-motyvatsiini skladovi kadrovoi bezpeky" [Social and motivational components of personnel security]. *Finansovyi prostir*, no. 2 (6) (2012): 44-51.

Poskrypko, Yu. A. "Mekhanizmy vdoskonalennia intelektualno-kadrovoi skladovoi ekonomichnoi bezpeky pidpryiemstv" [Mechanisms to improve the intellectual and human resources component of economic security]. *Naukovi zapysky UNDIZ*, no. 2 (22) (2012): 118-120.

Shtamburh, N. V. "Skladovi ekonomichnoi bezpeky pidpryiemstva" [Components of economic security]. *Biuleten Mizhnarodnoho Nobelivskoho ekonomichnoho forumu*, no. 1 (4) (2011): 490-496.

Tomanevych, L. M. "Kadrova bezpeka pidpryiemstva iak ob'iekt teoretychnoho doslidzhennia" [Personnel security of enterprise as an object of theoretical research]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Seriia ekonomichna*, no. 1 (2009): 185-192.

Voloshchuk, L. O., and Nekipelova, Yu. A. "Intelektualna skladova ekonomichnoi bezpeky pidpryiemstva" [The intellectual component of economic security]. http://economics.opu.ua/files/science/2014/ipredV_2014/43.pdf

УДК 65.011.1

ФОРМУВАННЯ СТРАТЕГІЇ АДАПТАЦІЇ ПІДПРИЄМСТВА ТОРГІВЛІ

© 2015 **РАЧКОВАН О. Д.**

УДК 65.011.1

Рачкован О. Д. Формування стратегії адаптації підприємства торгівлі

Метоюстаттієобґрунтуваннянеобхідностірозробкистратегіїадаптаціїпідприємствдомінливогосередовищафункціонуванняіметодичногопідходудоїїформуваннязурахуваннямспецифікиторговельноїгалузі. Обґрунтовано необхідність постійних змін діяльності підприємства відповідно до умов навколишнього середовища. У цьому контексті пропонується методичний підхід до формування стратегії адаптації підприємства торгівлі, де стратегічний процес розглянуто за послідовністю його здійснення на підприємстві з визначенням ключових етапів. Як можливі стратегічні альтернативи виокремлено: стратегію активної адаптації, стратегію консервативної адаптації та стратегію ситуаційної адаптації підприємств. Запропонований підхід дозволяє своєчасно реагувати на зміну навколишнього середовища і враховує зв'язок змін факторів навколишнього середовища з результуючими показниками діяльності торговельного підприємства.

Ключові слова: *стратегія адаптації, мінливе середовище, стратегічний процес, управління, підприємства торгівлі.*
Бібл.: *8.*

Рачкован Ольга Дмитрівна *– завідувачка Навчально-консультаційного центру, Харківський державний університет харчування та торгівлі (вул. Клочківська, 333, Харків, 61051, Україна)*
E-mail: *emfil@mail.ru*

УДК 65.011.1

Рачкован О. Д. Формирование стратегии адаптации предприятия торговли

Целью статьи является обоснование необходимости разработки стратегии адаптации предприятий к непостоянной среде функционирования и методического подхода к ее формированию с учетом специфики торговой отрасли. Обоснована необходимость постоянных изменений деятельности предприятия в соответствии с условиями окружающей среды. В этом контексте предлагается методический подход к формированию стратегии адаптации предприятия торговли, где стратегический процесс рассмотрен в последовательности его осуществления на предприятии с определением ключевых этапов. Как возможные стратегические альтернативы выделены: стратегия активной адаптации, стратегия консервативной адаптации и стратегия ситуационной адаптации предприятий. Предложенный подход позволяет своевременно реагировать на изменения окружающей среды и учитывает связь изменений факторов окружающей среды с результирующими показателями деятельности торгового предприятия.

Ключевые слова: *стратегия адаптации, изменяющаяся среда, стратегический процесс, управление, предприятия торговли.*
Библ.: *8.*

Рачкован Ольга Дмитриевна *– заведующая Учебно-консультационного центра, Харьковский государственный университет питания и торговли (ул. Клочковская, 333, Харьков, 61051, Украина)*
E-mail: *emfil@mail.ru*

UDC 65.011.1

Rachkovan O. D. Establishing an Adaptation Strategy of Trading Enterprise

The article is aimed at substantiation of the need for developing a strategy for adapting enterprises to the unstable environment of functioning and a methodical approach to its establishing in view of specificity of trade industry sector. The necessity of constant changes in the activity of enterprise in accordance with the conditions of the environment has been substantiated. In this context, a methodical approach to the formation of an adaptation strategy of trading enterprise has been proposed, where strategic process is considered in the sequence of its implementation at the enterprise together with identifying the key stages. As possible strategic alternatives has been allocated the following: active adaptation strategy, conservative adaptation strategy and situational adaptation strategy of enterprises. The proposed approach allows to opportunely respond to changes in the environment and takes into account the relationship of changes of environmental factors with the resulting indicators of performance of trading enterprise.

Key words: *adaptation strategy, changing environment, strategic process, management, trading enterprises.*
Bibl.: *8.*

Rachkovan Olga D. *– Head of Training and Consulting Center, Kharkiv State University of Food Technology and Trade (vul. Klochkivska, 333, Kharkiv, 61051, Ukraine)*
E-mail: *emfil@mail.ru*