

напрямів розвитку, які в найбільшій мірі сприятимуть досягненню успіху на зовнішньому ринку та пошуку оптимальних варіантів вдосконалення управління зовнішньоекономічною діяльністю підприємства. Також, для ефективного розвитку зовнішньоекономічної діяльності, підприємство повинно постійно досліджувати існуючі та потенційні ринки, з метою виявлення нових перспективних закордонних партнерів, можливостей розширення мережі збуту та проникнення на нові ринку збуту і заповнення їх новим товаром, а також визначення потенціалу продажу та ємності ринку.

Список джерел інформації

1. Гринишин Г. Методика аналізу зовнішньоекономічної діяльності підприємств / Г. Гринишин // Проблеми теорії та методології бухгалтерського обліку, контролю та аналізу. Сер. Бухгалтерський облік, контроль і аналіз. – 2014. – № 1 (28). – С. 64.

2. Овсієнко А. Управління зовнішньоекономічною діяльністю суб'єктів господарювання / А. Овсієнко // Економічний вісник університету. – 2015. – № 27/1. – С. 126–127.

О.М. Мартин, канд. екон. наук, доцент (*ЛДУБЖД, Львів*)

М.О. Живко, канд. юр. наук (*Солонківська СР*)

І.Р. Верещак, магістр (*ЛьвДУВС, Львів*)

А.Р. Верещак, магістр (*ЛьвДУВС, Львів*)

ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІЗАЦІЇ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ

Сьогодні тяжко уявити собі життя без комп'ютера, адже інформаційні технології настільки широко ввійшли в буденні справи кожного громадянина, що без них вирішення питань в «екстремному режимі» практично не можливі. Комп'ютеризація передачі інформації робить наше життя простішим і досконалішим. Інформаційні технології скрізь, як на місцях навчання чи роботи, так і дома, як у великих промислових центрах, так і забутій глибинці. Адже в умовах електронного світу не треба витратити зайвий час на рутинні операції, які можуть бути автоматизовані. Зокрема, система пошуку клієнтури, придбання чи реалізації товарів (послуг), дистанційне навчання у навчальних закладах, ознайомлення з новинами з усього світу, спілкування за допомогою електронної пошти та у режимі реального часу, участі у міжнародних та республіканських науково-практичних

заходах тощо сьогодні без труднощів можна здійснити за допомогою системи Інтернет.

Тобто, людина без зайвих витрат, переїздів, зміни місця праці може брати участь в різних розробках, наукових проєктах, працювати над колективними проєктами тощо.

Звідси, комп'ютерні технології вирішують важливі проблеми не лише окремих осіб чи груп людей, забезпечують їх комплексом інструментів, здатних автоматизувати розв'язання широкого діапазону проблемних питань та складних завдань, допомагають групуванню та плідній роботі колективів, вирішують проблему комунікації, впливають на прийняття рішень.

Проте, поряд з перевагами інформаційних технологій викреслюється ціла низка загроз втрати цінної інформації, яка може призвести до занепаду організації, ліквідації важливого проєкту чи безпеки держави загалом.

Входження України в інформаційне суспільство потребує наукового обґрунтування тенденцій та явищ, зокрема, нового змісту такої складової суспільних відносин, як інформаційна безпека в умовах інформатизації стосовно захисту інформації від злочинних посягань. Адже, інформаційні системи мають у собі приховану небезпеку. В процесі передавання даних в інформаційні бази можуть бути вторгнення, «зломи», тобто несанкціонований доступ сторонніх осіб, які можуть нанести шкоду державі, особам чи організаціям, в тому числі використати у злочинних намірах. Зокрема, можна розшифрувати дані, що передані електронною поштою, отримати електронні документи, кошти, підробити підпис тощо.

Щоб сформувану найпростішу базу загальної теорії організації інформаційної безпеки щодо захисту інформації, треба визначити методологічні аспекти та взаємозв'язки з іншими науковими дисциплінами. Тобто, ми розглядаємо теорію критичної маси інформації, на основі якої визначається тенденція, що в комплексі складає наукову дисципліну, що виникла на межі поєднання технічних і гуманітарних наук: правової інформатики, інформаційного права та тектології (теорії організації соціальних систем) [1-3].

Тобто, за природою свого походження інформаційна безпека має триєдиний зміст, що доповнюється і у перспективі буде доповнюватися спеціальними знаннями з інших галузей, підгалузей, інституцій технічних та суспільних наук, а це передбачає наявність визначення елементів системи та осмислення проблематики предметної галузі загалом.

При формуванні системи захисту інформації виникає необхідність застосування методів інтеграції та агрегації складових системи, її підсистем, що стає можливим при адаптації до предметної області теорії алгоритмізації, моделювання, теорії систем.

Пошук інформації в Україні не заборонений законом, тобто збирати інформацію може кожен суб'єкт господарювання чи громадянин, зокрема при умові – не використовувати заборонених методів, що порушують гарантовані Конституцією права і свобода людини.

Про бізнес-структури можна дізнатися 90-95% правдивої та корисної інформації з цілком легальних джерел: з Інтернету, з друкованих засобів масової інформації, під час проведення професійних семінарів, конференцій, виставок тощо [4].

Важливою проблемою є визначення конкретних факторів, які потрібно враховувати, щоб охарактеризувати безпеку бізнесу, тобто наявність як конкретної інформації в організації, їх засоби або технології, а також всю інформацію загалом по фірмі.

Для цього потрібно виходити з функціонального призначення систем, суб'єктів та об'єктів інформації, яка знаходиться на підприємстві. Головне завдання полягає у реалізації безпеки інформаційних процесів. А звідси головною цінністю є та інформація, яка обробляється в цих системах, та ким вона обробляється. Таким чином, захищеність інформації на підприємстві має забезпечувати безпеку інформації чи інформаційних ресурсів, що підлягають опрацюванню від «потенційно або реально можливих дій, що спричиняють несанкціонований або неправомірний доступ».

Для правильного прийняття управлінських рішень треба враховувати такі важливі фактори, як інтенсифікація розвитку інформаційних технологій, інформаційної економіки та інформаційного суспільства. Саме вони зумовили те, що підприємництво можна представити у вигляді інформаційної матриці, компонентно і структурно адекватної складній соціально-економічній системі, що формується в Україні [5]. Відношення до інформаційних технологій розвитку підприємництва як до органічної складової суспільної системи передбачає їх розгляд у єдності з персоналом, який продукує та застосовує ці технології. Для опрацювання інформації в автоматичному режимі необхідний високотехнологічний штат проектувальників та допоміжного персоналу [5].

Отже, комплексне забезпечення інформаційної безпеки має включати: охорону безпосередньо об'єктів зв'язку; наявність ліцензування підприємницької діяльності і сертифікація товарів і послуг

у цій сфері; правовий захист, що забезпечує захист інформації на правовій основі; організаційний захист, регламентуючий виробничу діяльність і взаємовідносини виконавців на нормативно-правовій основі; інженерно-технічний захист, що попереджає заподіяння шкоди інформації.

Список джерел інформації

1. Гавловський В.Д. Загальна теорія організації інформаційної безпеки щодо захисту інформації в автоматизованих системах від злочинних посягань. URL: <http://www.crime-research.ru> (вхід 25.06.2019)

2. Живко З.Б. Визначення бюджету на створення і утримання комплексної системи економічної безпеки підприємства: інформаційно-аналітичний аспект. *Актуальні Проблеми Економіки*. № 11(149), 2013. С.206-214 (624 с.).

3. Живко М.О., Босак Х.З. Захист інформаційних ресурсів у сфері інформації. *Управління розвитком. Збірник наукових статей*. № 15. Харків: Вид-во ХНЕУ, 2008. С.20-21.

4. Марущак А. Протидія злочинним та конкурентним механізмам доступу до інформації про суб'єкта господарювання. Сайт юридичного журналу „ЮСТІНІАН”. URL: <http://www.justinian.com.ua> (вхід 25.06.2019)

5. Живко З.Б., Данилович-Кропивницька М.Л. Інформаційна основа прийняття стратегічних управлінських рішень. *Актуальні проблеми економіки*, № 10, 2008. С. 69-80.

М.Е. Матвєєв, канд. екон. наук, доц. (*НЛТУ України, Львів*)

В.С. Ковальський, студент (*НЛТУ України, Львів*)

ЕМОЦІЙНА КОМПЕТЕНТНІСТЬ КЕРІВНИКА ЯК ОДИН З ІНСТРУМЕНТІВ УПРАВЛІННЯ ПОТЕНЦІАЛОМ ПЕРСОНАЛУ В ГОТЕЛЬНО-РЕСТОРАННОМУ БІЗНЕСІ

Однією з функцій управління підприємством є ефективне поєднання праці та капіталу з метою реалізації інтересів засновників. Підвищення ефективності використання персоналу стає ключовим ресурсом, що дозволяє готельно-ресторанному бізнесу успішно розвиватись й приносити прибутки. На сьогодні до персоналу приділяється особлива увага. Трудовий потенціал працівника – це здатність досягати конкретних результатів, вдосконалюватись, вирішувати поставлені завдання. Одним із можливих способів, що