УДК 658.5.012.1

Сотниченко В. М.
кандидат педагогічних наук, доцент,
професор кафедри менеджменту
Державного університету телекомунікацій (м. Київ)

Sotnychenko V. M.
Candidate of pedagogical Sciences,
Associate Professor, Professor of the
Department of management
State University of telecommunications (Kyiv)

ОРГАНІЗАЦІЙНО-МЕТОДОЛОГІЧНІ ЗАСАДИ АДАПТИВНОЇ СИСТЕМИ ЗАХИСТУ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНОГО ПІДПРИЄМСТВА

ORGANIZATIONAL AND METHODOLOGICAL FRAMEWORK OF ADAPTIVE SYSTEM TO PROTECT THE ECONOMIC SECURITY OF A TELECOM COMPANY

Анотація. У статті розглянуто організаційно-методологічні засади адаптивної системи захисту економічної безпеки. Урізноманітнення загроз потребує нового підходу до захисту економічної безпеки телекомунікаційного підприємства. Запропоновано організаційну структуру з трьох контурів: детекторного, ідентифікаційного та адаптивного. Така структура дає змогу працювати із загрозами більш організовано і по етапах. Кожен контур виконує свою функцію. Детекторний контур виявляє загрозу. Ідентифікаційний – визначає зміст, характер загрози та її спрямування. Адаптивний контур завершує роботу із загрозою.

Ключові слова: адаптивна система захисту, ризики, економічна безпека, розмірність загроз, цифровізація суспільства, трансформація, людський ресурс, технології, програмно-апаратне забезпечення.

Постановка проблеми. Актуальність питання щодо забезпечення надійного захисту економічної безпеки телекомунікаційного підприємства зумовлена тим, що саме з безпечного функціонування підприємства починає вибудовуватися система економічної безпеки телекомунікаційної галузі, народногосподарського комплексу країни і держави у цілому.

Успішно й якісно вирішити завдання забезпечення надійного захисту економічних інтересів телекомунікаційного підприємства неможливо без створення системи управління ризиками. Головним функціональним призначенням такої системи повинна бути здатність:

– оперативно реагувати на структурно-організаційні, змістові та якісні зміни середовища функціонування;

– протидіяти внутрішнім та зовнішнім факторам деструктивного впливу на результати діяльності підприємства;

– відтворювати ресурси життєдіяльності;

– здійснювати саморегулювання;

– зберігати тривалий час здатність до продуктивної діяльності в несприятливих умовах функціонування тощо.

У складних умовах сьогодення суб'єкти господарювання намагаються вирішувати питання захисту власних економічних інтересів за допомогою традиційних прийомів, методів та підходів. Багатократне застосування одного й того ж арсеналу сприяє створенню стереотипу, який використовується недоброчесними конкурентами, партнерами і, зрештою, зловмисниками.

Стереотип господарської поведінки дає їм змогу побудувати модель механізму несанкціонованого доступу до ресурсів підприємства, його фондів, активів для їх привласнення у злочинний спосіб. Через це реально постає потреба в пошуку та впровадженні таких менеджерських рішень, які б максимально повно й ефективно давали змогу прогнозувати розвиток телекомунікаційних підприємств на майбутнє, визначати та управляти тими ризиками, які створюють реальну загрозу для економічної безпеки підприємства. Сьогодні стан справ на українських телекомунікаційних підприємствах такий, що єдиного підходу до забезпечення економічної безпеки немає.

Аналіз останніх досліджень і публікацій. Комплекс телекомунікаційних підприємств України за видами діяльності, характером надання послуг і технологіями виробництва має досить широкий спектр. Це не лише послуги мобільного та фіксованого зв'язку, Інтернету, передачі інформації, навігації, геолокації тощо. Є ще тисячі телекомунікаційних підприємств, які займаються виробленням програмно-апаратного продукту, виготовленням і технічним обслуговуванням магістрального обладнання, технічним супроводженням і профілактикою ІТ-інфраструктур підприємств. Через це і завдання підготовки єдиних рекомендацій до створення такої системи захисту для всіх телекомунікаційних підприємств представляється надзвичайно складним. Кожне окреме підприємство працює за своєю унікальною системою й у вирішенні проблеми економічної безпеки потребує індивідуального підходу.

Проблеми забезпечення економічної безпеки, а також залежність економічної безпеки від низки зовнішніх і внутрішніх факторів представлені у роботах Л.В. Абалкіна, А.А. Беспалька, В.Ф. Гапоненка, О.А. Груніна, С.О. Груніна, В.М. Єсипова, А.Р. Ілларіонова, В.О. Карачаровського, А.В. Козаченка, В.І. Мунтіяна, В.П. Пономарьова, А.Н. Ляшенко та ін.

Визначення природи та параметрів ризиків як основи у формуванні загроз для економічної безпеки присвячено роботи Дж.М. Кейнса, О. Моргенштейна, Ф. Найта, Дж. фон Неймана. Чимало уваги було приділено й питанням прогнозування ризиків та способів управління ними в роботах таких авторів, як Р.М. Качалова, Е.Е. Куликова, А.В. Романюк, В.Ю. Харчук.

Дослідження проблеми управління ризиками, у тому числі підприємств та організацій, відображені в роботах

В.Т. Балабанова, І.В. Домінова, В.А. Москвіна, С.А. Корезина, В.С. Романова, Р.Г. Сніщенко. Концептуалізація принципів управління ризиками підприємства як інструменту в системі забезпечення його економічної безпеки отримала відображення у порівняно невеликій кількості наукових праць. У сучасній економічній науці представлені фундаментальні роботи у сфері теорії управління ризиками підприємств, описового інструментарію управління фінансовими ризиками в контексті фінансового менеджменту та методів економіко-математичного моделювання. Так, у роботах А.С. Кошечкіна, Е.Е. Куликової, Т.Б. Кузенко, А.А. Лобанова, В.М. Гранатурова, В.О. Шевчук, С.А. Філіна, О.С. Циганової розглядаються методи і способи управління ризиками в системі ризик-менеджменту.

Виділення невирішених раніше частин загальної проблеми. Тим не менше, є фактори, механізми, цілі, завдання, принципи і технології, що об'єднують на єдиній платформі всі телекомунікаційні підприємства незалежно від характеру та виду їх діяльності. В основі діяльності всіх телекомунікаційних підприємств є об'єднуючи цілі, завдання і принципи. Щодо об'єднуючих цілей, то вони розглядаються через призму завдань цифровізації суспільства, переходу до цифрової економіки. Кожен елемент цієї системи як результат продуктивної діяльності кожного окремого телекомунікаційного підприємства являє собою втілення і реалізацію на матеріальному, технологічному рівнях цих цілей і завдань.

Кожен вид усвідомленої і технологічно розробленої продуктивної діяльності має своє «дерево цілей». «Вирощено» це «дерево» на основі одного з головних наукових принципів – принципу збереження розмірності. Кожне телекомунікаційне підприємство залежно від характеру та виду діяльності має свої унікальні параметри її кінцевих результатів. Підприємство, що виготовляє антенні пристрої, матиме свої параметри, оператори зв'язку – свої унікальні параметри, телекомунікаційні підприємства з виготовлення устаткування – свої, підприємства сервісного обслуговування – свої. Всі ці параметри мають свою специфічну й унікальну розмірність. І ставити їх в один ряд за ознаками розмірності не можна, у них різні системи виміру.

Строго слідуючи принципу розмірності, можна розробити і побудувати свою однорозмірну систему захисту економічної безпеки кожного окремого телекомунікаційного підприємства або групи споріднених за видами діяльності підприємств. І це не суперечить основному завданню – створенню системи захисту економічної безпеки кожного окремого телекомунікаційного підприємства. А виходячи з того, що всі підприємства в межах галузі зведені в систему на основі єдиної магістральної мети – цифровізації суспільства і забезпечення переходу до цифрової економіки, – повинна бути й єдина система захисту економічної безпеки, де всі б різнорозмірні параметри результатів їхньої діяльності гармонічно і безконфліктно поєднувалися.

Для того щоб максимально ефективно вирішити завдання розроблення основ і створення такої системи захисту економічної безпеки всіх телекомунікаційних підприємств незалежно від характеру і виду їх діяльності, необхідно визначити такі фактори впливу, які б для всіх названих підприємств мали рівносильне значення.

Мета статті полягає у спробі визначити основні організаційно-методологічні підходи до створення адаптивної системи захисту економічної безпеки телекомунікаційного підприємства.

Виклад основного матеріалу дослідження. Вирішенням цих завдань науковці і практики займаються не один рік і вже мають певні науково-практичні напрацювання. Найбільш близьким напрямом дослідження в контексті зазначеного завдання є науковий пошук у плані встановлення залежності економічної безпеки від зовнішніх та внутрішніх факторів. Очевидно, що фактори впливу апріорі не можуть бути проігноровані підприємством, мова може йти тільки про силу такого впливу та наслідки; про те, на які вузли та механізми бізнес-процесів впливають ці фактори. Фактори впливу, за великим рахунком, не залишаються поза увагою будь-якого об'єкту господарювання, які об'єднані магістральною метою загальнодержавного характеру, оскільки вони породжують ризики для діяльності підприємства [1, с. 69–75]. Ризики, народжувані зовнішніми і внутрішніми факторами впливу, будуть різнитися між собою за такими знаковими параметрами:

– векторною спрямованістю;
– ймовірністю і силою впливу;
– рівнем актуальності у часі і просторі;
– здатністю до трансформації.

На сучасному етапі модернізації системи управління бізнес-процесами відбувається перехід від системи надзору та контролю до системи управління ризиками. І тому питання створення ефективно діючої системи управління ризиками є актуальним і для телекомунікаційних підприємств у тому числі.

Більш повно визначити сутність економічної безпеки телекомунікаційного підприємства можна з позицій її багатомірності. Це означає, що з погляду даного підходу економічна безпека складається з безлічі елементів і структурних зв'язків, що мають нелінійний характер. Маються на увазі фактори економічної безпеки, а саме: система управління підприємством; система управління потоками інформації та її захисту; інноваційна діяльність; управління персоналом; фінансові та інвестиційні потоки; екологічна, соціальна та політична ситуація в конкретному регіоні та в країні у цілому [2, с. 117–124; 3, с. 63–69]. Список можна продовжувати за більш докладного вивчення проблеми. Очевидним у цьому аспекті розгляду питання є те, що перераховані фактори для системи захисту економічної безпеки є одночасно й об'єктами захисту, й напрямами впливу ризиків.

Максимально результативно за такого підходу буде працювати адаптивна система захисту економічної безпеки. У цьому плані на основі спостережень за еволюцією біосистем можна робити очевидний висновок про те, що вони зберігали життєздатність і розвивалися завдяки тому, що швидко адаптувалися до змін середовища, в якому перебували. Відсутність адаптивної властивості неминуче призвела б до їх знищення.

Середовище, в якому працюють телекомунікаційні підприємства, є складним утворенням і постійно змінюється в різних площинах своєї структури: соціальній, політичній, економічній, екологічній, технологічній, політичній (рис. 1). Окрім того, самі підприємства постійно змінюються. А залежно від видів і профілю діяльності зміни також мають свій специфічний характер, природу, властивості та параметри. Отже, система захисту економічної безпеки телекомунікаційного підприємства повинна мати у своїй основі адаптивну структуру, здатну максимально адекватно реагувати на виклики середовища незалежно від їх розмірності, природи і характеру.

Здебільшого дослідники розглядають лише один аспект взаємодії підприємства з оточуючим середовищем. Звідси й позиція, що зовнішнє середовище впливає на роботу підприємства і потенційно несе в собі загрозу для його економічної безпеки. Виходячи із цього, розробляються підходи, принципи, прийоми, методи і техно-

логії захисту від потенційно можливих негативних впливів оточення на роботу підприємства. Зазвичай моделі захисту економічної безпеки вибудовуються конструктивно в межах технологічної і організаційної моделі безпосередньо підприємства. А розглядати питання захисту економічної безпеки на прикладі телекомунікаційного підприємства – це й сучасно, й перспективно, оскільки за цифровою економікою майбутнє. І в принципі в такому підході концептуальної помилки немає.

Технологічний ресурс телекомунікаційної галузі на сучасному етапі розвинутий настільки, що без перебільшення можна говорити про те, що телекомунікаційні підприємства активно впливають на формування оточуючого середовища [4, с. 81–88]. Каналів впливів достатньо для того, щоб змінювати характеристики і параметри оточення. Окреслимо лише деякі з них:

– часові характеристики суб'єкт-об'єктної взаємодії: сучасні продукти діяльності телекомунікаційних підприємств суттєво зменшили час на вирішення життєвих питань;

– просторові характеристики: все більш доступними стають різні сфери життєдіяльності людини, суспільства і держави, що значно збільшує можливості і варіанти організації продуктивної взаємодії на різних рівнях;

– енергозатратність: телекомунікаційні підприємства результатами своєї діяльності дають змогу значно скоротити обсяги енергозатрат на вирішення питань продуктивної взаємодії на особистому рівні, суспільному, державному і міждержавному;

– продуктивність: завдяки прогресивному розвитку і масштабному втіленню в життя інформаційно-телекомунікаційних технологій збільшується маса суспільнокорисного продукту, виробленого за одиницю часу.

Це лише деякі аспекти через які можна розглядати вплив результатів продуктивної діяльності телекомунікаційного підприємства на оточуюче середовище. Звичайно, що воно змінюється, і ці зміни, своєю чергою, впливають на функціонування телекомунікаційного підприємства.

Отже, можна зробити висновок, що розглядати проблему захисту економічної безпеки телекомунікаційного підприємства треба з урахуванням активної взаємодії підприємства з оточуючим середовищем. При цьому телекомунікаційне підприємство не лише впливає на середовище, а й помітно його змінює. Тобто своєю діяльністю телекомунікаційне підприємство бере безпосередню участь у формуванні зовнішніх факторів впливу на себе, у продукуванні ризиків.

Задається питання: чи може телекомунікаційне підприємство через результати власної діяльності впливати на рівень захищеності своєї економічної безпеки? Така можливість не виключається, оскільки на результати своєї продуктивної діяльності, які можна розглядати як провокативні виклики, підприємство логічно і закономірно отримує відповіді від оточуючого середовища. Оточуюче середовище треба сприймати й оцінювати як систему з усіма властивостями і належними їй параметрами і характеристиками. Система завжди реагує на зовнішні виклики. Реагує адекватно. Тобто які виклики, такі й відповіді. Багато в чому загрози економічній безпеці телекомунікаційного підприємства – це закономірний продукт діяльності самого підприємства.

Якщо розглядати характер і результати діяльності телекомунікаційного підприємства з погляду прогресу, то вона заслуговує тільки на позитивну оцінку. Якщо ж розглядати готовність українського суспільства до сприйняття нових умов існування і життєдіяльності в рамках нової прогресивної моделі з відповідними моральними принципами, то схвальну оцінку дати важко.

Дисонанс між телекомунікаційним прогресом і неготовністю українського суспільства до сприйняття «комфорту і затишку» цифрового життя й є головною причиною проблеми, пов'язаної з економічною безпекою телекомунікаційних підприємств.

Тепер щодо можливих варіантів вирішення проблемного поки ще питання щодо захисту економічної безпеки телекомунікаційного підприємства. Напрошуються два варіанти.

Перший. Підприємствам телекомунікації працювати на рівні готовності українського суспільства до адекватного і безконфліктного сприйняття його результатів і перспектив розвитку на шляху цифровізації з усіма наслідками. У такому разі рівень провокативності викликів буде нівелюватися на рівні готовності суспільства безконфліктно сприймати результати діяльності підприємства. І

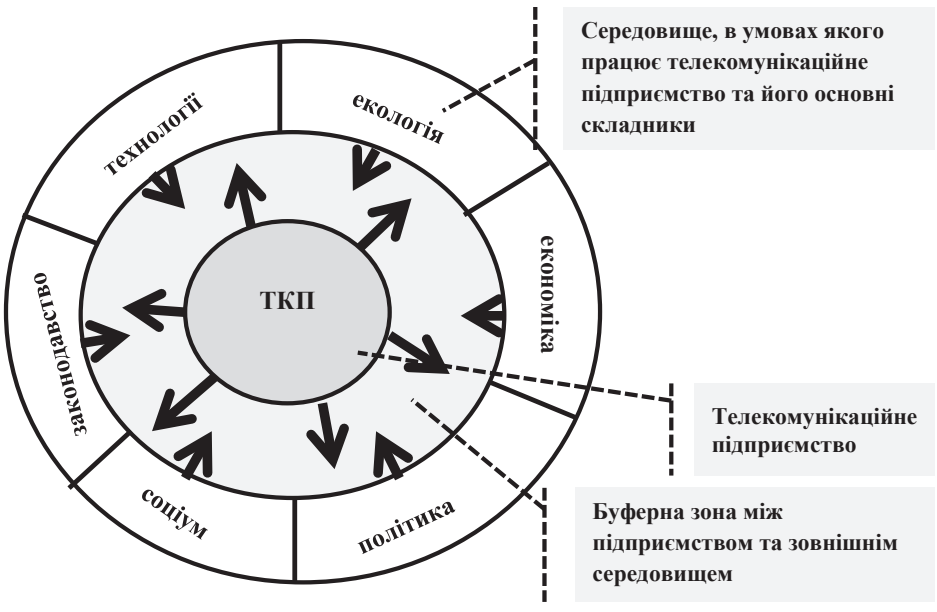

Рис. 1. Схема взаємодії телекомунікаційного підприємства із зовнішнім середовищем

реакції-відповіді з боку суспільства не будуть загрожувати економічній безпеці підприємства. Але тоді треба мати на увазі, що ми так і не зможемо інтегруватися у світову економіку на паритетних засадах, у нас і так із цим сьогодні багато проблем.

Другий варіант. Орієнтуватися не на рівень готовності суспільства до сприйняття інформаційно-телекомунікаційного прогресу, а включити програму тотальної підготовки суспільства до інформаційного прориву, передусім через реформування змісту освіти. Вважати неприпустимим, коли учні, студенти, слухачі володіють «цифрою» краще за вчителів, викладачів, професорів. Унеможливити займати ключові посади у сфері державного управління для тих людей, які на високому рівні не володіють інформаційно-телекомунікаційними технологіями. Це необхідно робити, незважаючи на очевидні втрати на першому етапі, інакше ми відстанемо назавжди [5, с. 30–35].

Українська інформаційно-телекомунікаційна система перебуває у стані конфлікту з європейським цифровим світом, який суттєво випереджає нас за рівнем технологічної готовності, а це означає, що українська економіка за таких обставин не тільки не буде розвиватися, а й постійно втрачатиме. Прикладів тому достатньо. Остання вірусна атака у червні 2017 р. показала, що найбільших утрат через це зазнала Україна: майже 75% від утрат усіх країн світу, що постраждали від цієї вірусної атаки. Цифра просто катастрофічна.

Тепер до питання про модель адаптивної системи захисту економічної безпеки телекомунікаційного підприємства. Між телекомунікаційним підприємством і середовищем, в якому воно перебуває, є зона, яку можна назвати буферною. У межах цієї зони відбувається контактна взаємодія двох сигнальних систем – підприємства й оточення. Підприємство як підсистема більш крупної системи на рівні державного масштабу не може функціонувати без контактів і зв'язків із системою, до складу якої воно входить. Характер взаємодії системи і підсистеми має особливості, зумовлені принципом ієрархічності, за яким система організована. З боку держави і суспільства є вимоги до підприємства, а з боку підприємства – результат його продуктивної діяльності та власне бачення характеру взаємодії й ролі самого підприємства у вирішенні завдань як тактичного, так і стратегічного масштабу.

Ці взаємодії в буферній зоні мають конфліктний характер. Це зумовлено багатьма причинами, серед яких можна назвати:

– домінуючий характер ставлення держави і суспільства до суб'єкта господарювання – телекомунікаційного підприємства;

– намагання підприємства мати власну позицію щодо власних виробничих, технологічних та організаційних можливостей;

– намагання державної системи втручатися у справи підприємства, контролювати бізнес-процеси і, за можливості, керувати ними;

– створення підприємством системи захисту конфіденційної інформації як від недоброчесних конкурентів, так і від органів державної влади;

– намагання держави контролювати фінансові потоки підприємства;

– прагнення підприємства до збільшення самостійності у вирішення питань власного стратегічного розвитку й організації продуктивної взаємодії з іншими суб'єктами господарювання як у рамках народногосподарського комплексу країни, так і за її межами.

Буферна зона – це простір, де передусім повинні вирішуватися питання організації конструктивної взаємодії між потенційними учасниками, зацікавленими сторонами. Це зона, де мають узгоджуватися протиріччя, вирішуватися спірні питання, вибудовуватися позиції, формуватися відносини. І, зрештою, це середовище, в якому формується система ризиків. І, напевно, не треба чекати, коли ці ризики, умовно кажучи, перетнуть усі можливі кордони телекомунікаційного підприємства і почнуть розвиватися й діяти на його території.

Скорочення дистанції між системою ризиків і потенційними об'єктами та предметами їх умотивованої уваги не сприяє підвищенню рівня економічної безпеки підприємства. Це призведе до того, що потенційні загрози реалізовуватимуть свій деструктивний для підприємства ресурс швидше і втрати будуть більшими. А тому логічно було б зробити висновок про те, що систему захисту економічної безпеки телекомунікаційного підприємства треба вибудовувати у буферній зоні.

Сучасна ж практика створення системи захисту економічної безпеки телекомунікаційного підприємства побудована на тому, що все це розробляється і функціонує на базі самого підприємства й у межах його життєвого простору. І система захисту починає діяти, коли виникає загроза, і починає вже діяти в межах цього простору. У світовій практиці є два популярних підходи до вирішення питань захисту економічної безпеки: реагування за фактом виникнення загрози і створення системи захисту завчасно. Перший підхід менш затратний, але більш ризикований, бо в разі потужної атаки можна втратити все. Хоча ризик може виправдатися й тим, що підприємство не буде піддано загрозам і все обійдеться, а до того часу можна чимало заробити. А якщо й буде напад, то ймовірні втрати можна компенсувати отриманими до цього доходами.

Другий підхід – це створення постійно діючої системи захисту економічної безпеки підприємства. Це значно дорожче за перший підхід, але несе в собі певні гарантії відносно безпечного функціонування телекомунікаційного підприємства.

Враховуючи різновимірність і природну неоднорідність параметрів факторів впливу на телекомунікаційні підприємства, виходимо на необхідність побудови особливої системи захисту економічної безпеки. Безумовно, завдання представляється зрозумілим і достатньо доступним для виконання, коли природа і вимірність загроз знаходяться в одній площині, в одній системі координат. Реально картина доволі складна і тенденції до її подальшого ускладнення чим далі посилюються разом з ускладненням та урізноманітненням світу, особливо що стосується його технологічного складника. Сподівання на те, що далі буде простіше вирішувати питання захисту економічної безпеки, не мають жодної перспективи. Зростаючи темпи цифровізації світу, масштаби поширення технологій Інтернету речей – це грандіозні виклику часу, відповідями на які вже є і зростають далі адекватні відповіді світу і людства у цілому у вигляді різноманітних за властивостями і потенційними можливостями системи ризиків.

Ризик – це економічна категорія і потенційно являє собою подію, яка може відбутися або не відбутися. Може призвести до отримання прибутку рівно як до втрат. Може не дати жодного результату – нульовий ризик. Ризиком можна управляти, але для цього необхідно знати, як і чим на нього впливати, щоб максимально повно спрогнозувати настання ризикової події, а вже потім приймати рішення по ньому для зниження ступеня ризикованості й отримати максимально вигідний для підприємства результат [6, с. 21–24; 7, с. 7–8].

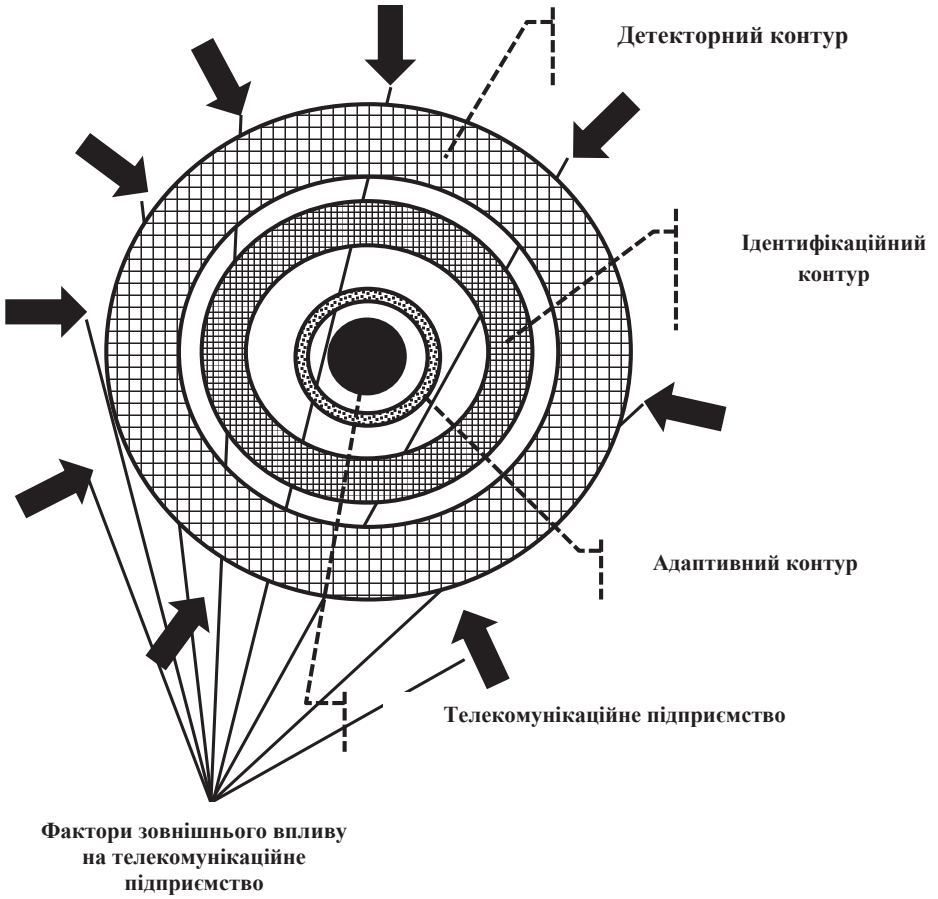

Рис. 2. Схема організації адаптивної системи захисту економічної безпеки телекомунікаційного підприємства

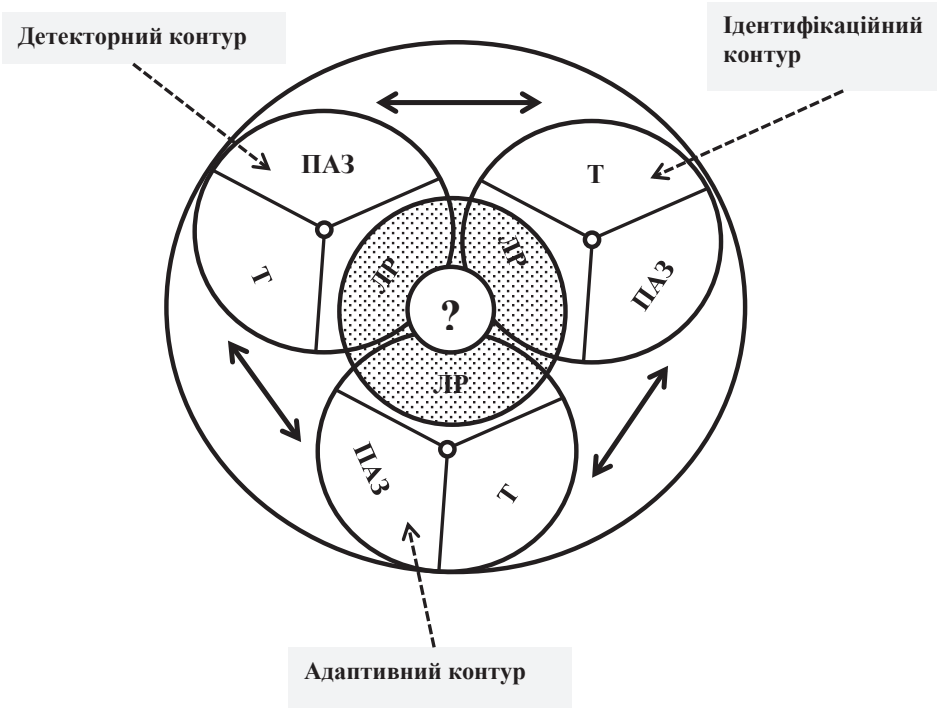

Рис. 3. Схема взаємодії між структурними складниками системи адаптивного захисту економічної безпеки телекомунікаційного підприємства: ЛР – людські ресурси, ПАЗ – програмно-апаратне забезпечення, Т – технології

Окрім того, що ризиками треба вміти ефективно управляти, необхідно ще знаходити технологічні рішення адаптації телекомунікаційних підприємств до нових умов функціонування. І, напевно, першочерговим є завдання створення системи захисту.

Очевидно, що найбільш надійною, адекватною й ефективною системою захисту в сучасних умовах і на перспективу може бути система адаптивна (рис. 2). Як підказує практика захисту економічної безпеки від ризикових дій із негативними наслідками і втратами, адаптивна система повинна мати три контури:

– детекторний;
– ідентифікаційний;
– адаптивний.

Названі контури являють собою систему з різнорідних і різновимірних елементів, а саме: людського ресурсу, програмно-апаратного забезпечення і технологій (рис. 3).

Кожен з елементів виконує притаманний лише йому комплекс функцій. У кожному з трьох контурів людський ресурс виконує соціальну ціннісно-орієнтовану функцію, необхідність реалізації якої зумовлена політико-правовим складником економічної безпеки телекомунікаційного підприємства. Цій функції притаманні суб'єктивні відтінки як результат суспільної реакції на динаміку змін системи соціальних цінностей і запитів, вимог та потреб, з урахуванням яких будуть формуватися управлінські рішення, команди та алгоритми соціальної поведінки. Отримати максимально, втратити мінімально: забезпечення реалізації такої установки є головним завданням системи адаптивного захисту економічної безпеки телекомунікаційного підприємства.

Практика в напрямі захисту економічної безпеки підприємства доводить, що реальних результатів можна досягти, коли вся система захисту консолідована на рівні організації ресурсної взаємодії.

Перший і найзначущіший рівень такої організації – це людські ресурси. Це саме той капітал, який являє собою концептуальну основу адаптивної системи захисту і потребує найбільших вкладень. Недоліки на цьому рівні організації ресурсної взаємодії негативно позначаються на результатах функціонування усієї системи. Символічний знак запитання на схемі вказує на те, що ціннісна основа організації взаємодії на рівні людського ресурсу є категорію динамічною і може змінюватися під впливом будь-яких обставин. Відповідно будуть змінюватися і технології, й інструмент їх реалізації – програмно-апаратне забезпечення. Саме цим пояснюються технологічні та інструментальні відмінності в організації життєдіяльності в різних цивілізаційних осередках.

Другий рівень організації ресурсної взаємодії – це взаємозв'язок між програмно-апаратним забезпеченням і технологіями. Технології відіграють домінуючу, активну роль. Поява нової технології потребує програмно-апаратної модернізації.

Отже, на першому рівні організації знаходиться людський ресурс, де формуються потреби, вимоги і прагнення до отримання життєво необхідного продукту. Пошуки шляхів і способів вирішення цього завдання призводять до народження нових технологій. Нові технології, своєю чергою, потребують програмно-апаратного забезпечення, здатного максимально повно реалізувати технологічний ресурс.

Висновки. Актуальність проблеми забезпечення рівня економічної безпеки телекомунікаційного підприємства має тенденцію до зростання. Це зумовлено ускладненням і вдосконаленням технологій, появою нових завдань у плані цифровізації економіки і нових ризиків, подальшою інтеграцією України в європейський та світовий простір тощо.

Традиційна одновимірна система захисту економічної безпеки телекомунікаційного підприємства, побудована на техніко-технологічній платформі, втрачає актуальність, оскільки не може ефективно протистояти новим загрозам, природа і характеристики яких динамічно змінюються. Свідченням цьому, наприклад, є катастрофічні наслідки для України вірусної атаки у червні 2017 р.

На перший план виходить завдання створення такої системи захисту економічної безпеки телекомунікаційного підприємства, яка була б здатною розпізнавати більш широкий спектр загроз у різних системах їх виміру і адекватно реагувати на їх появу в зоні економічних інтересів підприємства.

Вирішити це завдання можливо шляхом створення нової, адаптивної системи захисту економічних інтересів телекомунікаційного підприємства. Така система повинна складатися з трьох контурів: детекторного, ідентифікаційного й адаптивного. Основу кожного з контурів становлять людський ресурс, технологічний і програмно-апаратне забезпечення.

Організація взаємодії ресурсів у кожному з контурів і в адаптивній системі захисту в цілому має ієрархічний порядок, домінуючу роль в якому відіграє людський ресурс.

Науковий інтерес представляє перспектива розвитку адаптивної системи захисту економічних інтересів телекомунікаційного підприємства в умовах зростання ролі інформаційно-комунікаційних технологій на шляху до цифрового суспільства.

Список використаних джерел:

1. Аванесова Н.Е. Державне рулювання процесів забезпечення економічної безпеки підприємств оборонної промисловості України. Інетелект XXI. 2017. № 2. С. 69–75.
2. Кузенко Т.Б. Стратегічні підходи до управління фінансовими ризиками підприємства. Інетелект XXI. 2017. № 2. С. 117–124.
3. Гудзь О.Є., Сотниченко В.М. Методологічний вимір формування стратегічного портфеля фінансової безпеки підприємства. Облік і фінанси. 2016. № 3(73). С. 63–69.
4. Зубко Т.Л. Оцінка рівня безпеки підприємства галузі зв'язку. Економіка. Менеджмент. Бізнес. 2016. № 3(17). С. 81–88.
5. Сотниченко В.М. Механізм управління економічною безпекою телекомунікаційного підприємства. Економічний вісник Запорізької державної інженерної академії. 2017. № 2-2(08). С. 30–35.
6. Білинська М.М., Малюська В.А. Розбудова спроможності державної служби до управління змінами для підтримки реформ в Україні: навчальний посібник для державних службовців. К.: Національна академія державного управління при Президентові України, 2016. 98 с.
7. Підхомний О.М. Фінансова безпека України: інструменти і стратегії формування: монографія. Львів: ЛНУ імені Івана Франка, 2014. 320 с.

Аннотация. В работе рассмотрены организационно-методологические основы адаптивной системы защиты экономической безопасности. Разнообразие угроз требует нового подхода к защите экономической безопасности телекоммуникационного предприятия. Предложена организационная структура из трех контуров: детекторного, идентификационного и адаптивного. Такая структура позволяет работать с угрозами более организованно и по этапам. Каждый контур выполняет свою функцию. Детекторный контур обнаруживает угрозу. Идентификационный – определяет содержание, характер угрозы и ее направления. Адаптивный контур завершает работу с угрозой.

Ключевые слова: адаптивная система защиты, риски, экономическая безопасность, размерность угроз, цифровизация общества, трансформация, человеческий ресурс, технологии, программно-аппаратное обеспечение.

Summary. In the article the organizational and methodological framework of adaptive system of protection of economic security. The diversity of threats requires a new approach to the protection of economic security of a Telecom company. The proposed organizational structure of the three circuits: detection, identification and adaptive. This structure allows to work with threats in a more organized and in stages. Each circuit performs its function. The detection circuit detects a threat. Identification – determines the content, the nature of the threat and its direction. Adaptive circuit – exits the program.

Key words: adaptive protection, risk, economic security, the dimension of the threats to the digitalization of society, transformation, human resource, technology, software and hardware.

УДК: 330.338.47

Старинець О. Г.
кандидат політичних наук,
доцент кафедри менеджменту
Державного університету телекомунікацій

Starynec O. G.
Ph.D in Politics
Department of Management
State University of Telecommunications

МЕТОДИ ФІНАНСОВОГО АНАЛІЗУ ДІЯЛЬНОСТІ ПІДПРИЄМСТВ У СИСТЕМІ АНТИКРИЗОВОГО УПРАВЛІННЯ

METHODS OF FINANCIAL ANALYSIS OF ACTIVITY OF ENTERPRISES IN SYSTEM OF ANTICRISIS MANAGEMENT

Анотація. У статті розкрито суть та значення фінансового аналізу діяльності підприємства. Розглянуто види фінансового аналізу. Наведено характеристику основних методів фінансового аналізу діяльності підприємства. Визначено переваги та недоліки окремих методів фінансового аналізу діяльності підприємств. Досліджено роль фінансового аналізу в системі антикризового управління підприємством.

Ключові слова: підприємство, фінансовий аналіз, методи фінансового аналізу, результати діяльності, антикризове управління.

Постановка проблеми. Сучасний етап розвитку економіки вимагає від підприємств постійного підвищення ефективності діяльності та зміцнення своїх позицій. Запровадження системи антикризового управління будь-якого підприємства є невід'ємною умовою його успішного функціонування. Питання застосування відповідних методів фінансового аналізу діяльності підприємств для формування механізму антикризового менеджменту набуває особливої актуальності в нинішніх умовах.

Аналіз останніх досліджень і публікацій. Сутність та особливості фінансової діяльності підприємства розглянуто в працях таких учених, як: І.О. Бланк, І.Т. Балабанов, В.В. Ковальов, М.Л. Котляр, С.М. Пясталов, Н.І. Строченко, Г.В. Савицька, В.В. Шиян та ін.

Виділення невирішених раніше частин загальної проблеми. Сьогодні важливо визначити найбільш ефективне поєднання методів фінансового аналізу для розроблення антикризового механізму управління підприємствами зв'язку.

Мета статті полягає в аналізі та обґрунтуванні окремих методів фінансового аналізу та їх ролі в антикризовому управлінні підприємством.

Виклад основного матеріалу дослідження. Для вирішення конкретних завдань фінансового аналізу застосовується ціла низка спеціальних методів, які дають змогу одержати кількісну оцінку окремих аспектів фінансової діяльності підприємства. Фінансовий аналіз використовує низку методів, як загальнонаукових і загальноекономічних, так і специфічних. Можна виділити серед них основні [1, с. 48]:

– горизонтальний аналіз;
– вертикальний аналіз;
– трендовий аналіз;
– метод фінансових коефіцієнтів;
– аналіз інвестиційної привабливості підприємства;
– порівняльний аналіз;
– факторний аналіз (у тому числі аналіз за схемою Дюпон-каскад).