УДК 346.24.658.5

Сотниченко В. М.
кандидат педагогічних наук, доцент,
професор кафедри менеджменту
Державного університету телекомунікацій

Sotnychenko V. M.
Candidate of Pedagogical Sciences,
Associate Professor, Professor, Chair of Management
State University of Telecommunications

ЕКОНОМІЧНА БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ: СТАН ТА ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМИ

THE ECONOMIC SECURITY OF TELECOMMUNICATION ENTERPRISES: STATUS AND SOLUTIONS TO PROBLEMS

Анотація. У статті розглянуто окремі аспекти економічної безпеки телекомунікаційних підприємств. Визначено основні складники економічної безпеки підприємств галузі. Наголошено на необхідності глибокого розуміння керівниками підприємств будь-якої галузи економіки сутності телекомунікаційних систем і технологій. Вказано на необхідність інтеграції гуманітарних і технічних знань. Накреслено основні шляхи у напрямі забезпечення захисту від загроз для економічної безпеки.

Ключові слова: економічна безпека, телекомунікаційні системи, складники економічної безпеки, телематика, мультимедійний продукт.

Постановка проблеми. Проблема як категорія характеризується насамперед тим, що потребує змін параметрів предмету розгляду з тим, щоб максимально нейтралізувати деструктивні фактори в тій галузі науки та практики, в межах якої цей предмет розглядається. Коли розглядаються деструктивні впливи на економічну безпеку телекомунікаційних підприємств, актуальним залишається питання запобіганням цим впливам з метою створення умов стабільного функціонування підприємства телекомунікації.

Аналіз останніх досліджень та публікацій. Питанням економічної безпеки взагалі приділяється значна увага, особливо на сучасному етапі. Наростання обсягів аналітичних матеріалів з проблем економічної безпеки починається з 90-х років минулого століття. А вже останні два десятиліття акцент робиться на диференціації цієї проблеми за галузями і напрямами економічної діяльності.

Зрушено з місця і питання економічної безпеки в телекомунікаційній галузі. Зумовлено це багатьма суттєвими чинниками, які знайшли відображення в результатах досліджень науковців. Так, наприклад, Л.В. Лозоренко вказує, в тому числі, на необхідність формування механізму управління розвитком персоналу у сфері мобільного зв'язку, який зможе більш повно і на професійному рівні враховувати специфіку галузі.

О.В. Карпенко, досліджуючи складники системи економічної безпеки, також стверджує, що рівень економічної безпеки підприємництва залежить від того, наскільки ефективно його керівництво і спеціалісти будуть спроможні уникнути можливих загроз і ліквідувати шкідливі наслідки окремих негативних складникыв зовнішнього і внутрішнього середовищ.

С.В. Бєлоусова пропонує чотири стратегії управління ризиками, такы як перенесення ризику на інших осіб; стратегія прийняття ризику на себе – полягає у покритті збитків за рахунок власних ресурсів; стратегія попередження збитків – зводиться до заходів, які застосовуються задля зменшення ймовірних втрат та мінімізації їх наслідків; стратегія уникнення ризику – свідоме рішення не наражатися на певний вид ризику.

О.Е. Гудзь, розглядаючи проблеми стратегічного інноваційного розвитку, доходить висновку, що інноваційні стратегії генерують додаткові загрози і створюють для управління підприємством складні умови: підвищений рівень невизначеності кінцевих результатів за строками, витратами, якістю й ефективністю; примноження інвестиційних ризиків проектів, особливо довгострокових; нарощення потоку управлінських та організаційних змін на підприємстві. Реалізація будь-якої інноваційної стратегії пов'язана з неминучістю перебудови управлінських структур підприємства, оскільки зміна в системі будь-якого елемента зумовлює зміни стану всіх інших. Це характерно для телекомунікаційної галузі, основний ресурс яких базується на впровадження новітніх технологій.

А дослідники І.В. Довба і С.Ю. Сойма важливим завданням вважають необхідність переорієнтації на новітню та високотехнологічну модель вдосконалення та розвитку бізнес-процесів, що відбуваються на підприємстві. Саме управління бізнес-процесами підприємства в межах реалізації стратегії розвитку дає змогу знайти напрями оптимізації та досягнення гнучкості у діяльності підприємства.

Торкаючись питання щодо невирішеної частини загальної проблеми, слід зауважити, що це зовсім не є свідченням того, що результати наукового доробку в галузі економічної безпеки не можуть транслюватися на діяльність підприємств телекомунікаційної галузі. Все більше і більше з часом з'являється науково опрацьованих елементів системи економічної безпеки, з яких вибудовуються системи, специфічні для телекомунікаційних підприємств. Але при цьому що далі, тим більш актуальним стає необхідність вивчати цю проблему на основі ґрунтовних знань про те, як працюють телекомунікаційні підприємства. Необхідне глибоке і професійне розуміння сутності телекомунікаційних систем і телекомунікаційних технологій.

Наприклад, набуває все більшого значення нова науково-технічна дисципліна – телематика, предметом якої є методи передачі інформації на відстані, які значно перевищують лінійні розміри площі, що зайняті учасниками зв'язку. Телематика – це ще й назва безпаперової технології, яка виключає використання носіїв інформації на проміжній стадії її обробки.

Отже, актуальним є питання максимального наближення рівнів гуманітарних і технічних знань, їх подальшої інтеграції. Це потребує виходу на нові методологічні підходи. За таких умов дослідження бізнес-процесів, побудованих на засадах сучасних телекомунікаційних систем і технологій, їх результати будуть мати сучасний характер і перспективу свого подальшого розвитку.

Метою статті є виділення ключових завдань і напрямів подальших наукових досліджень у сфері економічної безпеки телекомунікаційних підприємств. Темпи розвитку і запровадження сучасних інформаційних технологій, динаміка розвитку та обсяги ринку інфокомунікаційних товарів і послуг потребують розроблення нових методологічних підходів для забезпечення гармонійного поєднання складників економічної безпеки підприємств телекомунікаційної галузі.

Виклад основного матеріалу дослідження. Питання безпеки ніколи не втрачають актуальності. Їх вивченню присвячена безліч фундаментальних досліджень, сотні монографій, написано тисячі статей. Традиційно питання розглядається через тріаду: безпека держави – безпека регіону – безпека підприємства. Це зрозуміло й логічно. По-перше, легко з'ясовується логіка класичної ієрархії. Змінюється лише напрям залежно від завдань дослідження цього питання: від безпеки держави до безпеки підприємства і навпаки. Це різні аспекти розгляду. А тому включаються відповідні механізми переходу від одного рівня безпеки до іншого на основі принципів взаємозв'язку, взаємозалежності і взаємозумовленості об'єктивних і суб'єктивних факторів.

Першопричиною появи загроз для економічної безпеки підприємств телекомунікаційної галузі можна назвати порушення рівноваги в класичному розуміння цього поняття. Підприємство представляє собою складну структуру, стабільна діяльність якої є можливою лише за умов, коли між його структурними складниками встановлена гармонійна рівновага. Система економічної безпеки також функціонує в оптимальному режимі, коли рівновага дотримана між її складниками: фінансовим, інтелектуально-кадровим, організаційним, ринковим, техніко-технологічним, політико-правовим, силовим тощо.

Технології, методи та прийоми забезпечення безпеки можуть бути найрізноманітнішими. Це залежить від того, у якій сфері життєдіяльності виникла загроза. Вони можуть бути застосовані як всередині структурної організації підприємства, так і за її межами. Можна, наприклад, закрити кордони. Організувати тотальний контроль і встановити відповідний режим. Створити спільну систему безпеки на партнерській основі. Розробити й впровадити високотехнологічні системи захисту. Увести строго регламентовану систему розподілу ресурсів. Заборонити певні види діяльності. І є ще багато інших способів забезпечення стану стабільного функціонування підприємства [1, с. 130–133].

Країни Західної Європи для забезпечення національної безпеки почали використовувати економічні методи. Намітилися два підходи до боротьби з погрозами безпеці взагалі й економічної зокрема. Перший з них полягає в тому, що загроза як фактор може й не з'явитися, і до її реальної появи ніяких заходів із посилення захисту економічної безпеки не впроваджується. Весь наявний ресурс підприємства використовується на забезпечення та розвиток бізнес-процесів. З появою загрози включається механізм локалізації проблеми та її подальшого усунення.

Інший підхід полягає в тому, щоб завчасно спрямувати зусилля на виявлення потенційних загроз і створення ефективних механізмів їх усунення. Вибудовується система захисту економічної безпеки підприємства, яка активізується у разі появи загрози. Такий підхід більш затратний, оскільки система захисту потребує до себе постійної уваги, підтримки на рівні ресурсозабезпечення, технічного і технологічного вдосконалення [2, с. 33–37].

І перший, і другий підходи цілком зрозумілі. Перший більше пов'язаний з ризиком втрат як для підприємства, так і для регіону або країни загалом. Але якщо все буде організовано грамотно, професійно й керівництво буде далекоглядним, тобто ймовірність того, що умови для виникнення погроз буде зведено до мінімуму, то будуть зекономлені ресурси. Ну, а якщо погроза виникне, то доведеться витратитися й передбачити можливість повторення, закріпивши набутий досвід.

Але ситуація може складатися по-різному. Обставини під впливом як внутрішніх, так і зовнішніх факторів можуть динамічно змінюватися, створюючи нестабільні умови для існування системи. Погрози виникають досить часто. І тоді другий підхід – профілактика можливих погроз на перспективу – є цілком виправданим. Важливим показником буде різниця між затратами на постійне утримання системи захисту і втратами від несанкціонованого втручання. Підприємство, яке буде реагувати на загрози по факту їх виявлення, може втратити значно більше, ніж те підприємство, яке завчасно побудувало систему захисту і утримувало її постійно.

У першій ситуації також є свої переваги. Економлячи на системі захисту, підприємство може більше вкладатися в розвиток бізнесу і отримувати більше доходів. З іншого боку таке підприємство буде більш привабливим для шахрайства.

Для характеристики економічної безпеки підприємства найчастіше використовуються показники фінансового становища й результатів його господарської діяльності. Тобто використовується стандартний інструментарій, а нові поняття не вводяться. Так само, як і не вводяться нові поняття цієї категорії.

Найпоширенішим визначенням економічної безпеки підприємства є стан його захищеності від негативного впливу на нього зовнішніх і внутрішніх факторів, які дестабілізують ситуацію. Природно, що для кожного окремого підприємства внутрішні фактори й погрози будуть мати сугубо індивідуальний характер. А от зовнішні можуть однаково деструктивно впливати на комерційні інтереси й цілі підприємства. Як відомо, це насамперед протиправна діяльність кримінальних структур, конкурентів, приватних осіб і організацій, які займаються промисловим шпигунством. А також шахрайство, неспроможність ділових партнерів, недбалість, безвідповідальність і непрофесіоналізм, навмисна бездіяльність, прояв корупції, конфліктні ситуації в колективі співробітників [3, с. 67–70; 4, с. 12–16].

Ознаками порушення економічної безпеки на підприємстві насамперед є видимі або відчутні зміни результатів його діяльності (як адміністративної, так і господарської), зміни режиму роботи, швидкості протікання різного роду процесів, зміна конфігурації, окремих параметрів тощо.

Все більше привертає уваги питання захисту економічної безпеки підприємств телекомунікаційної галузі. Причина зрозуміла: усі сучасні бізнес-процеси реалізуються на основі телекомунікаційних систем та інфор-

маційних технологій, стрімко розвивається електронна комерція. Підприємства сьогодні не можуть обійтися без наявності власної ІТ-інфраструктури. Ця галузь динамічно розвивається, оскільки з'являються нові технології, які дають змогу отримувати більший економічний ефект [5, с. 26–32]. Одночасно з цим ІТ-інфраструктури підприємств і телекомунікаційні підприємства є найбільш вразливими, незахищеними. Практика доводить, що система захисту послаблюється під час структурних змін і технічних переобладнань.

Прикладів ефективного використання ІТ-інфраструктур для успішного розвитку бізнесу достатньо. Наприклад, компанія Alibaba. Її клієнтами є мільйони покупців і продавців з усього світу. Використовуючи сучасні телекомунікаційні системи й технології, компанія дає постачальникам можливість зв'язатися з покупцями з усього світу, а покупцям – зручні інструменти пошуку товарів і партнерів для бізнесу. Масштаби колосальні: у каталозі понад 400 мільйонів товарів, покупці й продавці з понад 190 країн світу. Асортимент товару – від промислового устаткування до одягу й предметів побуту. І незалежно від того, наскільки клієнт компанії впевнено орієнтується в сучасних мобільних технологіях, компанія завжди знаходить можливість йому допомогти.

Компанія, будучи великою платформою в електронній комерції, постійно розвивається технологічно, залучає для розвитку бізнесу новітні досягнення в галузі телекомунікаційних систем і технологій бізнесу. А в червні 2016 року на Міжнародному економічному форумі в С.-Петербурзі засновник компанії Alibaba Джек Ма запропонував проект створення «електронного шляху» за аналогією з «шовковим шляхом». Це вже інтегрований мегапроект розвитку міжнародного економічного співробітництва на основі сучасних досягнень в галузіі телекомунікацій. Але водночас успішні компанії, що ефективно використовують ІТ-ресурс, є привабливими для шахрайства, яке також успішно розвивається на організаційному і техніко-технологічному рівнях.

Підприємства телекомунікацій – це підприємства, що надають послуги з використанням магістральних транспортних систем. При цьому надання телекомунікаційних послуг не супроводжується видимими змінами на рівні інфраструктури, не відбувається фізичного переміщення матеріальних ресурсів, немає видимих змін матеріальних цінностей. А якщо такі зміни й будуть мати місце, то виявити їх і оцінити втрати можна тільки за допомогою спеціальних програм діагностування.

Телекомунікаційні підприємства надають різні види послуг. Неправильно було б вважати, що це винятково послуги зв'язку. Перелік послуг, крім зв'язку, досить широкий: програмно-апаратне забезпечення, встановлення устаткування, сервісне обслуговування тощо. Процес надання кожного з видів послуг знаходиться в полі зору шахрайства. Це зумовлює створення системи захисту для кожного окремого виду діяльності, хоча всі ці процеси відбуваються у телекомунікаційній галузі.

Але головна послуга, яку надає телекомунікаційне підприємство, полягає в переміщенні мультимедійного продукту споживачеві. І саме на цій лінії діяльності підприємства найчастіше виникають проблеми, пов'язані зі швидкістю доставки продукту кінцевому споживачеві. Можуть виникнути погрози безпосереднього негативного впливу на сам переданий продукт, на його конфігурацію й зміст. Можуть бути найрізноманітніші причини. Ну, приміром, фактори зовнішнього впливу можуть бути спрямовані на безпосередньо транспортну систему, якою користується телекомунікаційне підприємство.

Сьогодні економіка України не може обходитися без телекомунікаційної галузі. І чим кращі технологічні параметри галузі, тим ефективніше працює економіка. Галузь розростається і вже охоплює практично всі систему народногосподарського комплексу держави. Сьогодні на ринку телекомунікацій працює понад 4,2 тис. операторів та провайдерів. Бізнес стає більш мобільним і, як наслідок, більш прибутковим. Кількість терміналів мобільного зв'язку в Україні у 2,5 раза перевищує кількість стаціонарних телефонів [6, с. 246–249]. Це тільки звичайний зв'язок із простими функціями комунікації. Але ж при цьому зростає кількість терміналів, які працюють під управлінням операційних систем. Тобто це багатофункціональні системи з достатньою потужністю, які надають користувачеві різнопланові інформаційні та телекомунікаційні послуги.

Паралельно із зростанням рівня технічного забезпечення бізнесу зростають і проблеми, пов'язані з його захистом. Першою серед них є несанкціоноване втручання в бізнес через канали інформаційно-телекомунікаційного забезпечення і несанкціоноване використання трафіку. На побутовому рівні – це все одно, що користуватися громадським транспортом і не сплачувати проїзд. Причому технологія незаконного використання трафіка не стоїть на місці, а поступово розвивається. І розвивається паралельно з розвитком телекомунікаційних систем і технологій.

Саме на це не можна не звертати уваги у плані оцінки можливої економічної небезпеки для підприємства. Якщо в ланцюжок діяльності підприємства з надання послуги зв'язку вбудовано кілька програм, то зрозуміло, що чим більше таких програм, тем вищий ризик можливих втрат через викривлення окремих параметрів переданої інформації. І це насамперед є питанням внутрішньої економічної безпеки, тому що така інформація доступна тільки співробітникам компанії. Так наприклад, керівник однієї з фірм завдав Белтелекому збитків на 2,8 млрд карбованців, заробляючи на незаконних послугах. Діючи з порушенням виняткового права національного оператора зв'язку, шахрай, використовуючи спеціальне устаткування, призначене здійснювати перетворення телефонного сигналу, виступив в ролі посередника з доставки міжнародного трафіка і пограбував національного оператора. Протягом півроку він незаконно одержав дохід у сумі більш 40 тисяч доларів. Це приклад звичайного шахрайства на телекомунікаційному підприємстві.

Розвивається телекомунікаційна галузь, і не відстає в розвитку телекомунікаційне шахрайство (понад 200 різновидів). Розвиток шахрайства стимулює роботу над створенням ефективних і надійних систем захисту. На створення систем захисту оператори витрачають величезні кошти, щоб запобігти навмисному несанкціонованому доступу до послуг зв'язку.

За різними джерелами, втрати від несанкціонованого доступу до послуг зв'язку у середньому становлять 5% від доходів. Що ж стосується вірогідності цих даних, то вони викликають сумніви. Досвідчений оператор не буде привселюдно повідомляти про свої втрати від шахрайства. По-перше, втрачає авторитет. По-друге, розкриває комерційну таємницю свого підприємства (свого роду антиреклама, і навряд чи це буде приваблювати клієнтів). По-третє, це дає можливість шахраю оцінити ефективність своєї «роботи» й удосконалювати методи.

Долати ці труднощі, пов'язані зі створенням системи захисту від несанкціонованого втручання, самотужки, на рівні використання індивідуального ресурсу суб'єктів господарювання – затратно і малоефективно.

А ефективно вирішити це питання можна централізовано, на державному рівні. В Україні взято курс на розбудову Національної телекомунікаційної мережі. Буде створено єдину державну спеціальну транспортну телекомунікаційну систему, яка працюватиме в інтересах державних органів, на захист державної безпеки й оборони, суб'єктів критичної інформаційної інфраструктури. Буде створено єдину державну систему захищених телекомунікаційних сервісів. За прогнозами економістів галузі, реалізація цього проекту дасть змогу за короткий термін (1–2 роки) майже втричі скоротити витрати бюджетних коштів на функціонування захищених інформаційно-телекомунікаційних систем в інтересах держави на шляху до цивілізованого європейського і світового суспільства.

Висновки. Проблема захисту економічної безпеки у сфері діяльності підприємств телекомунікаційної галузі вже давно набула світових масштабів і потребує остаточного вирішення у найближчій перспективі, оскільки представляє ідеологію «злодіїв у законі», що прагнуть жити за рахунок інших. Одним з основоположних принципів міжнародного права, та й національних систем права також, є справедливість. Цей принцип рівною мірою є важливим і цінним у всіх сферах життєдіяльності суспільства й держави, і його треба неухильно дотримуватися, щоб уникнути порушення рівноваги як фактору економічної безпеки.

Одним із напрямів утримання балансу у сфері економічної безпеки підприємств телекомунікаційної галузі є максимальне зближення рівнів гуманітарного й технічного знання як науковців, так і практиків-підприємців. Враховуючи те, що без власної ІТ-інфраструктури будь-які підприємства на сучасному етапі, а тим більше на перспективу обійтися не можуть, питання економічної безпеки для них так само актуально за змістом, характером, структурою і наслідками, як і для підприємств телекомунікаційної галузі. У зв'язку з цим набуває наукового інтересу визначення методологічних підходів щодо створення універсальної системи захисту від загроз для економічної стабільності всього народногосподарського комплексу.

Список використаних джерел:

1. Довба І.В., Сойма С.Ю. Особливості оптимізації управління бізнес-процесами підприємства та методи їх удосконалення [Електронний ресурс] / І.В.Довба, С.Ю. Сойма // Науковий вісник Мукачівського державного університету. Серія: Економіка. – 2016. – Випуск 6. – С. 130–133. – Режим доступу: http://www.economyandsociety.in.ua/journal/6_ukr/22.pdf.
2. Лозоренко Л.В. Аналіз ринку мобільного зв'язку України та напрями його розвитку [Електронний ресурс / Л.В. Лозоренко // Науковий вісник Миколаївського національного університету імені В.О. Сухомлинського. – 2017. – Випуск 15. – С. 246–249. – Режим доступу: http://global-national.in.ua/issue-15-2017/23-vipusk-15-lyutij-2017-r/2768-lazorenko-l-v-analiz-rinku-mobilnogo-zv-yazku-ukrajini-ta-napryamki-jogo-rozvitku.
3. Лозоренко Л.В. Модель соціальної відповідальності підприємств мобільного зв'язку / Л.В. Лозоренко // Науковий вісник Херсонського державного університету. Серія: Економічні науки. Випуск 22-2/2017. Частина 2. – С. 12–16 .
4. Бєлоусова С.В. Формування програми управління фінансовими ризиками підприємства / С.В. Бєлоусова // Міжнародні економічні відносини та світове господарство. Науковий вісник Ужгородського національного університету. – 2017. – № 12. – С. 33–37.
5. Гудзь О.Є. Гармонізація механізму стратегічного управління інноваційним розвитком підприємства [Електронний ресурс] // Глобальні та національні проблеми економіки. – 2015. – № 3. – С. 26–32. – Режим доступу: http://global-national.in.ua//.
6. Карпенко О.В. Складові системи економічної безпеки підприємництва / О.В. Карпенко // Науковий вісник Херсонського державного університету. Серія: Економічні науки. Випуск 9/2014. Частина 6. – С. 67–70.

Аннотация. В статье рассмотрены отдельные аспекты экономической безопасности телекоммуникационных предприятий. Определены основные составляющие экономической безопасности предприятий отрасли. Отмечена необходимость глубокого понимания руководителями предприятий любой области экономики сущности телекоммуникационных систем и технологий. Указано на необходимость интеграции гуманитарных и технических знаний. Намечены основные пути в направлении обеспечения защиты от угроз экономической безопасности.

Ключевые слова: экономическая безопасность, телекоммуникационные системы, составляющие экономической безопасности, телематика, мультимедийный продукт.

Summary. The article considers some aspects of economic safety of telecommunication enterprises. The main components of economic security of enterprises of the industry. The necessity of a deep understanding of business leaders in any field of the economy entities of the telecommunication systems and technologies. The necessity of the integration of humanitarian and technical knowledge. The main ways to ensure protection against threats to economic security.

Key words: economic security, telecommunications systems, components of economic security, telematics, multimedia product.