УДК 338.246.8

Сотниченко В.М.
кандидат педагогічних наук, доцент,
Державний університет телекомунікацій

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ОЦІНКИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ

METHODOLOGICAL APPROACHES TO THE ASSESSMENT OF ECONOMIC SECURITY OF TELECOMMUNICATIONS PROVIDERS

АНОТАЦІЯ

В статті розглядаються окремі аспекти розвитку телекомунікаційної галузі в Україні. Показано тенденції в економічній безпеці підприємств. Наводяться статистичні дані щодо розвитку галузі. Вказується на необхідність проведення реформ. Вказується на застарілу законодавчу базу. Пропонується методологічна модель розбудови системи економічної безпеки в телекомунікації.

Ключові слова: інформаційно-комунікаційні технології, діагностика загроз, економічна безпека, програмний продукт, незадекларовані функції, конвергентні мережі.

АННОТАЦИЯ

В статье рассматриваются отдельные аспекты развития телекоммуникационной отрасли в Украине. Показано тенденции в экономической безопасности предприятий. Приводятся статистические данные по развитию отрасли. Указывается на необходимость проведения реформ. Указывается на устаревшую законодательную базу. Предлагается методологическая модель развития системы экономической безопасности в связи.

Ключевые слова: информационно-коммуникационные технологии, диагностика угроз, экономическая безопасность, программный продукт, незадекларированные функции, конвергентные сети.

ANNOTATION

The article discusses some aspects of the development of the telecommunications industry in Ukraine. Displaying trends in economic security companies. Statistical data on the development of the industry. The necessity of reform. Specify on outdated legal framework. The methodological model of economic security in communications.

Keywords: information and communication technologies, Diagnosis threats, economic security, software, undeclared function, converged networks.

Рівень економічної безпеки є категорією динамічною і змінюється в процесі функціонування підприємства під впливом багатьох факторів, серед яких важливе місце посідає фактор технологічний. Розвиток телекомунікаційних технологій та застосування найкращих досягнень в бізнес-процесах сприяє підвищенню рівня економічної безпеки: більш досконалі технології – більш високий рівень захисту. В першу чергу, це характерно для телекомунікаційних підприємств, на результатах діяльності яких найбільш помітно відбивається вплив технологічного фактору [3, с. 26-27].

Постановка проблеми. На сучасному етапі розвитку телекомунікацій намітилась тенденція до того, що підприємства галузі стають все більше захищеними завдяки розвитку нових технологій. Виникає запитання: як рівень економічної безпеки телекомунікаційного підприємства впливає на рівень економічної безпеки підприємств в суміжних сферах, діяльність яких вони забезпечують технологічно? Як будуть захищені ті підприємства, які використовують телекомунікації в бізнесі? І як продавці послуг телекомунікацій будуть нести відповідальність, якщо з їхньої вини буде спричинено збитки через порушення системи економічної безпеки? Це питання на сучасному етапі набуває все більшої актуальності. А суть проблеми в тому, що, за оцінками експертів, в Україні недостатня технологічна готовність [1, с. 18], некомпетентне державне регулювання, застарілі технології, а це негативно впливає на обсяги інвестицій [2, с. 14].

Аналіз останніх досліджень і публікацій. Аксіомою світу сучасного, минулого й майбутнього є встановлена історичним досвідом людства пряма залежність перспективи майбутнього від реалій сьогодення. Що буде закладено сьогодні, проявиться завтра конкретними результатами. Стосується ця прописна істина всіх галузей і напрямів життєдіяльності як окремої людини, так і суспільства в цілому. Виходячи із загальної і класичної установки на позитивний результат всіх суб'єктів цього процесу, оптимізації його результатів і подальшого покращення умов свого існування, отримуємо висновок про солідарність інтересів і, на їхній основі, узгоджених і консолідованих дій.

Значну увагу вивченню питання економічної безпеки приділили в своїх працях такі відомі автори, як Барановський А.О., Батова В.Н., Гудзь О.Є., Гапоненко В.Ф., Єпіфанов А.О., Мунтіян В.І., Новикова І.В., Папєхін Р.С. Слід зазначити, що названі автори в своїх дослідженнях акцентують на фінансовій безпеці, що, без сумніву, є важливою для телекомунікаційного підприємства. Однак тут є досить специфічні особливості, пов'язані зі специфікою галузі. І це представляє науковий інтерес.

Виділення невирішених раніше частин загальної проблеми. Оскільки світ є ієрархічним, то й організація продуктивної діяльності його суб'єктів відбувається на кожному конкретному рівні його структурного утворення. І на кожному рівні побудовано свою систему збереження умов стабільного існування та розвитку. Така система потребує для свого гарантованого існування надійної системи захисту. В цьому немає нічого нового, ідея має глибоке історичне

коріння. Але актуальність цього питання має далеку перспективу свого розвитку, доки існує світ і людство в розмаїтті аспектів і напрямів свого розвитку. Специфіка підприємств, що працюють в галузі телекомунікацій, пов'язана, в першу чергу, із характером послуг і технологій їх надання, які дуже швидко змінюються за структурою, якістю і змістом [4, с. 82]. Причому, телекомунікації активно присутні у всіх секторах економіки. А спектр інструментів та можливостей формується і створюється в середині самої галузі.

Мета статті. Основною метою цієї статті є необхідність загострити увагу на актуальних для галузі питаннях, які потребують реформування. Галузь розвивається швидкими темпами, зростає кількість працівників та робочих місць.

За даними Комітету Верховної Ради України з питань інформатизації та зв'язку, кількість співробітників галузі до 2020 року зросте до 300 тисяч, робочих місць у суміжних сферах – до 400 тисяч, а надходження до державного бюджету становитимуть 300 млрд грн. Очевидно, у звязку із цим галузь потребує реформування на функціональному, адміністративному і законодавчому рівнях. Це лише загальна інформація для роздумів. А якщо взятися більш професійно, то на сьогодні наша країна, через недостатню увагу до розвитку галузі, знаходиться у дуже небезпечному становищі: зростає загроза протистояння в інформаційному просторі. На сьогодні майже 20 країн світу мають все необхідне для ведення кібервійни, і Російська Федерація у цьому списку не на останньому місці. Ще у 2013 році там утворено підрозділ ФСБ з інформаційної боротьби, розбудовуються війська інформаційних операцій.

Це на рівні національної безпеки [5, с. 79]. З іншого боку, загрозу може створювати і програмний продукт іноземного походження, який використовується в управлінні підприємством. Експертам галузі добре відомо, що в такому продукті можуть бути незадекларовані і приховані функції.

Тема безпеки завжди на першому плані і завжди актуальна. Виникає загроза – актуалізується питання безпеки. На її забезпечення потрібні ресурси. А ресурси, як відомо, є універсальною категорією з конкретними можливостями задоволення всіх запитів з усіх напрямів життєдіяльності людини, суспільства і держави. Вони не є безмежними. І якщо кількість ресурсів збільшується в одному місці, то зменшується в іншому. Таким чином, чим більше загроз, тим більше ресурсів використовується на їх подолання і тим менше їх залишається для задоволення потреб життєдіяльності, надання необхідних послуг.

Однак, слід зауважити, що рівень захищеності від загроз є категорією динамічною і змінюється як в «часі», так і в «просторі». Мається на увазі рівень технологічного розвитку середовища, в якому з необхідністю реалізуються певні технології, сфера та умови діяльності – простір.

Виклад основного матеріалу дослідження. Цікавою є тенденція, яка намітилася у взаємодії різних за призначенням і завданнями суб'єктів господарювання. Найбільш характерно це для телекомунікаційного підприємства, з одного боку і, наприклад, торговельного підприємства з іншого. Для телекомунікаційного підприємства рівень безпеки тим вище, чим менша ймовірність несанкціонованого доступу до його баз даних, мереж. Для торговельного підприємства також є актуальною ця проблема, але більшу небезпеку складають втрати від злодійства, шахрайства, порушення техніки безпеки, недобросовісної конкуренції, недостатній рівень професіоналізму персоналу тощо.

Послуги, яких потребує суспільство на сучасному етапі, мають доволі широкий спектр, одним з найбільших серед них є телекомунікаційні послуги, забезпечувані відповідними підприємствами. Кількість користувачів, так само як і їх категорій, неухильно зростає. Види і характер послуг також зростають залежно від рівня організації продуктивної діяльності – від окремої людини (на рівні задоволення власних потреб) до транснаціональних корпорацій.

Сучасне економічне середовище на рівні галузей і окремих підприємств консолідовано за цілями і завданнями: рентабельність – прибуток – домінування – монополія [6, с. 78-80]. Що ж стосується методів їх досягнення, то вони мають доволі широкий спектр, який залежить від багатьох чинників. Наприклад, ступінь відповідності чинному законодавству, їх легітимність, чесність і відкритість, толерантність і солідарність у намірах і діях тощо. В тому числі це стосується і телекомунікаційних підприємств, які піддаються впливу безлічі внутрішніх і зовнішніх загроз.

В умовах неоднозначності протікання соціально-економічних процесів і різноманітності способів і варіантів реалізації управлінських рішень підвищення ефективності діяльності й конкурентоспроможності залежить від системи оцінки й керування економічною безпекою підприємства [6, с. 33-34].

Для телекомунікаційних підприємств, що забезпечують роботу ринку інфокомунікаційних послуг, питання економічної безпеки є особливо актуальним. Причин тут декілька. Наприклад, швидкий розвиток і застосування сучасних телекомунікаційних технологій потребує розробки і запровадження відповідних (адекватних) систем їх захисту. Для її розробки і запровадження потрібні ресурси. А ресурси задіяно для забезпечення основного функціонування підприємства. Тобто, необхідно перерозподіляти ресурси, відволікати їх від основних процесів. Перерозподіл ресурсів повинен відбуватися за певною методикою і на технологічній основі з тим, щоб не допустити деструктив-

них проявів в роботі підприємства. Контроль за перерозподілом ресурсів повинен тривати до того моменту, поки відновлена система захисту не забезпечить безпечне функціонування підприємства. На це потрібен час. І цей час може бути використаний конкурентами не на користь цього телекомунікаційного підприємства.

Вирішення завдань управління економічною безпекою компанії пов'язано з цілою низкою труднощів: визначення загроз за видами, параметрами, ступенем безпеки, джерелом виникнення, способів і механізмів їх нейтралізації та подальшого знищення тощо. Не меншого значення мають питання, що пов'язані з визначенням виробничих ресурсів, необхідних для реалізації дій по організації управління економічною безпекою підприємства.

Для того, щоб завдання управління економічною безпекою підприємства було вирішено максимально ефективно, необхідно попередньо вирішити кілька важливих завдань, а саме:

– розробити методи діагностики наявності загроз та передумов їх виникнення;

– розробити механізми захисту підприємства від загроз;

розробити механізми профілактики та нейтралізації загроз;

– розробити систему управління економічною безпекою підприємства.

І, що найбільш важливо, всі перелічені вище алгоритми і механізми треба звести в систему на єдиній платформі і з єдиним центром управління. Очевидно, що методи діагностики і механізми захисту діяльності підприємства від загроз ще не гарантують його безпеки. Повинна бути розроблена, випробувана і запущена у постійному режимі система управління економічною безпекою, яка буде автоматично активувати всі перелічені вище модулі в залежності від актуальності у вирішенні того чи іншого завдання.

В першу чергу, в постійному режимі повинен працювати механізм діагностики на предмет появи ймовірної загрози. Для виявлення безлічі факторів прояву загрозливих ситуацій повинні бути систематизовані й класифіковані ймовірні загрози, сформований методичний апарат виявлення й оцінки загроз, розроблені процедури керування ними. В основі виявлення і оцінки потенційної тяжкості загроз у телекомунікаційного підприємства повинні бути розроблені якісні методи оцінювання і на їх основі складена матриця загроз з тим, щоб скоротити час на її усунення або ж знищення.

Отримавши сигнал про появу загрози, діагностичний модуль визначає її основні характеристики, серед яких найважливішими є вектор та сила загрози, час активної дії, можливі наслідки її дії для економічної безпеки підприємства. Далі, методика діагностики повинна передбачати вироблення рекомендацій для модулів профілактики, захисту, нейтралізації (знищення) загрози і видавати такі рекомендації для практичної реалізації.

Результатом відпрацювання всіх рекомендованих дій по захисту від загрози підприємства повинен бути алгоритм, який має зберігатися в базі даних системи управління економічною безпекою телекомунікаційного підприємства. Алгоритм повинен мати таку структуру, яка дозволила б його час від часу вдосконалювати, модернізувати, тобто, адаптувати до змін. Методика ж діагностики повинна мати механізми прямої взаємодії з базою даних алгоритмів і, у випадку виникнення загрози, активізувати необхідний алгоритм.

Процес дослідження виникнення загроз та їх вплив на економічну безпеку телекомунікаційних підприємств потребує приділення особливої уваги специфіці їх діяльності. Особливість полягає в тому, що підприємство працює на ринку інфокомунікаційних послуг, де попит превалює над пропозиціями послуг, які виробляються в мережевому режимі[1, 19; 6, 78-80]. Тому доречно на початковому етапі дослідження виділяти особливі, профільні загрози для безпеки підприємства, виходячи з того, що підприємство надає послуги, які здебільшого виробляються в мережевому режимі, що суттєво відрізняє його від інших типів бізнесу. Це і потребує першочергової уваги, оскільки дозволить на початковому етапі аналізу звести коло досліджуваних загроз до тих з них, які прямо і безпосередньо впливають на роботу підприємства. Це сприятиме заощадженню ресурсів і навіть дозволить створити певний запас.

Для підприємства пріоритетним є мінімізація загроз, які виникають або можуть виникнути в ході техніко-виробничих процесів [1, 18; 2, 15-16]. Причинами цього може бути кілька факторів, серед яких на перших позиціях стоять організаційно-виробничий, професійний, технологічний. При чому, технологічний фактор впливу на економічну безпеку телекомунікаційного підприємства має дуже динамічний характер. Можна наводити велику кількість прикладів, як і з якими темпами розвиваються телекомунікаційні технології в бізнесі, але найбільш переконливим аргументом може бути те, що буквально протягом десяти днів (8 листопада в м. Бішкек, Казахстан і 17-18 листопада 2016 року в м. Києві на базі Державного університету телекомунікацій) один за одним відбулися два Регіональні форуми Міжнародного союзу електрозв'язку, на яких розглядалися питання забезпечення сталого розвитку інформаційно-комунікаційних технологій, тенденції розвитку конвергентних мереж з використанням технологій 4G і 5G. Вже сьогодні очевидно, що подальший розвиток конвергентних мереж найближчим часом зробить найбільший вплив на бізнес.

Разом з тим, як вже згадувалося, загрози для цього типу підприємства пов'язані із загрозами для інших типів бізнесу, оскільки сьогодні важко знайти бізнес, який би обходився без послуг телекомунікацій – систем або тех-

нологій. І цей зв'язок також становить інтерес для дослідження.

На сьогодні, серед дослідників загроз для економічної безпеки підприємства немає єдиної точки зору щодо визначення їх поняття. Це тільки підкреслює актуальність проблеми, її наукове значення і перспективність вивчення. Відсутність єдиної наукової позиції щодо поглядів на проблему є гарантією того, що інструментарій боротьби із загрозами обіцяє бути різноманітним, а методологія – придатною для управління економічною безпекою підприємства.

Висновки. Загроза для економічної безпеки телекомунікаційного підприємства, яке займається виробленням і наданням інфокомунікаційних послуг є потенційно можливою подією, яка може викликати негативні наслідки для підприємства у результаті реалізації свого деструктивного потенціалу.

Крім того, що загроза є потенційною подією, певною мірою передбачуваною, вона може представляти собою і несприятливий збіг певних обставин з такими ж негативними для підприємства наслідками. Але збіг обставин – це не стихійне явище, а закономірний результат процесу визрівання потенційних загроз, який не був завчасно виявлений. Це ще раз вказує на необхідність створення такої системи управління економічною безпекою, яка б дозволяла не лише вчасно нейтралізувати загрози, але й відстежувати їх зародження на ранньому етапі.

Загрози для економічної безпеки підприємств, залежно від обставин і умов розвитку бізнесу, можуть бути викликаними різними причинами і мати різні джерела (осередки) виникнення, різну природу. Безумовно, вони потребують впорядкування, систематизації, класифікації. Ця аналітично-організаційна робота має кілька рівнів складності і глибини, що залежить від завдань дослідження. Для вирішення цього завдання буде достатньо простої і зрозумілої класифікації загроз для економічної безпеки підприємства, а саме:

– за причинами:

вмотивовані і цілеспрямовані;

невмотивовані, нецілеспрямовані;

– за цілями і завданнями:

орієнтовані на конкретну деструктивну дію;

не мають конкретної мети, орієнтовані в цілому на завдання шкоди підприємству;

– за терміном дії:

довготривалі;

короткотривалі;

– за спрямуванням:

одновекторні;

багатовекторні;

– за джерелами (осередками) виникнення:

в межах підприємства за рахунок внутрішніх ресурсів;

за межами підприємства – зовнішнє джерело виникнення.

Наведена класифікація може бути використана для створення платформи для розміщення на ній системи управління економічною безпекою підприємства.

Багато в чому всі вище перелічені критерії систематизації, впорядкування загроз зумовлюються тенденціями розвитку економіки. Стосується це, в першу чергу, тих джерел, де загрози формуються вмотивовано і цілеспрямовано. Тенденції і є векторами, що вказують на конкретні цінності і пріоритети суб'єктів економічної діяльності. І тому, здебільшого, загрози створюються спеціально, цілеспрямовано, з конкретними завданнями, мають спеціально розроблену структуру і орієнтовані на знищення конкуренції.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України: матеріали парламентських слухань у Верховній Раді України 3 лютого 2016 р. / Верховна Рада України, Комітет з питань інформатизації та зв'язку; ред. кол.: О.І. Данченко (голова), Г.О. Андрощук, О.Г. Старинець, О.А. Баранов [та ін.]. – К.: Парлам. вид-во, 2016. – 256 с.
2. Кириллов И. Украинский рынок ИТ: жизнь после революции // Сети &Бизнес. – 2014. – №1(74). – С. 14-20.
3. Гудзь О.Є. Гармонізація механізму стратегічного управління інноваційним розвитком підприємства [Електронний ресурс] // Глобальні та національні проблеми економіки. – 2015. – №3. – Режим доступу: http://global-national.in.ua. – С. 26-32.
4. Зубко Т.Л. Оцінка рівня економічної безпеки підприємства галузі зв'язку / Зубко Т.Л. // Економіка. Менеджмент. Бізнес. – №3(17) 2016. – К.: ДУТ, 2016 – С. 81-87.
5. Макаренко Т.Є. Стратегія забезпечення інвестиційної безпеки малого та середнього бізнесу в Україні (на прикладі франчайзингу) / Макаренко Т.Є. // Науково-аналітичний щоквартальний збірник Національного інституту стратегічних досліджень «Стратегічні пріоритети». – Київ, 2016 – Випуск №1(38) – С. 78-85
6. Новикова І.В. Управління конкурентоспроможністю телекомунікаційних підприємств: теорія, методологія, практика: монографія / И.В. Новикова. – Миколаїв: ФОП Швец В.Д., 2013. – 296 с.