8. Тупкало В.Н. Методика формирования системы сбалансированных показателей оценки эффективности управления предприятием / С.В.Тупкало, В.Н. Тупкало // Системи управління, навігації та зв'язку: зб. наук. пр. - К.: ЦНДІНУ, 2011. - Вип. 3(19). - С.169 – 175.
9. Тупкало В.М. Контролінговий механізм реалізації бізнес-стратегії підприємства // В.М. Тупкало // Економіка. Менеджмент. Бізнес: зб. наук. пр. – К.: ДУТ. – Вип.1(11), 2015.- С.5-14.
10. Тупкало В.М. Основи методології процесного бізнес – моделювання Тупкало. / В.М. Тупкало // Економіка. Менеджмент. Бізнес: зб. наук. пр. – К.: ДУТ. – Вип.2(12), 2015.- С.5-15.

Тупкало Виталий Николаевич. Менеджмент – аудит процессно-ориентированных предприятий: проблема и методологические аспекты. *Изложены авторские элементы научно-методического аппарата менеджмент - аудита процессно-ориентированных предприятий на основе контроллингових правил выделения, композиции и наглядного (графического) представления системы бізнес-процессов с использованием языка процессного моделирования TML.*

Ключевые слова: *менеджмент – аудит, процессно-ориентированное управление, бізнес-инжиниринг.*

Tupkalo Vitaliy. Management – the audit process-oriented enterprises: the problem and methodological aspects. *It sets out the elements of the author's scientific and methodical device management – the audit process-oriented enterprises on the basis of the rules controlling selection, composition and visual (graphical) representation of business systems-processes using the process modeling language TML.*

Keywords: *management – audit, process-oriented management, business-engineering.*

УДК 346.24.658.5

Гудзь О.Є., д.е.н., проф.,
Сотниченко В.Н., к.пед.н., доц.,
Державний університет телекомунікацій

ЕКОНОМІЧНА БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ: ПРОЯВИ ЗАГРОЗ ТА ЇХ УНИКНЕННЯ

У статті розглядаються питання виникнення погроз для економічної діяльності телекомунікаційних підприємств. Розглядаються причини й ознаки появи погроз, механізми їх реалізації, способи незаконного використання трафіка оператора.

Ключові слова*: економічна безпека, погроза безпеки, шахрайство, прояви корупції, права національного оператора.*

Постановка проблеми. Проблема як категорія, характеризується, в першу чергу, 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. У даному випадку, коли розглядаються деструктивні впливи на економічну діяльність телекомунікаційних підприємств, актуальним залишається питання запобіганням цим впливам з метою створення умов для економічної безпеки підприємства телекомунікації.

Аналіз останніх досліджень та публікацій. Питанням економічної безпеки взагалі приділяється, особливо на сучасному етапі, значна увага. Починаючи з 90-х років минулого

століття в Україні починається наростання обсягів аналітичних матеріалів, присвячених дослідженнню питань економічної безпеки. Початок, можна вважати, з виходом у світ підручника «Економічна безпека держави» за авторством Г.Пастернак-Таранушенка. Зрушено з місця актуальне і болюче питанная економічної безпеки, яке в різних аспектах розглядалося в роботах таких вчених як В.Андрійчук, І.Бінько, О.Барановський, О.Власюк, Б.Губський, Р.Дацків, Т.Ковальчук, О.Користін та інші авторитетні дослідники цього питання, яке з часом набуло статусу наукової проблеми.

Невирішена раніше частина загальної проблеми. 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 зявляється науково опрацьованих елементів системи економічної безпеки, з яких вибудовуються системи специфічні для телекомунікаційних підприємств. Але, при цьому, очевидно, що далі, тим більш очевидним стає необхідність вивчати цю проблему на основі грунтовних знань про те, як працюють телекомунікаційні підприємства. Глибокого і професійного розуміння сутності телекомунікаційних систем і телекомунікаційних технологій.

Виклад основного матеріалу. На разі набуває все більшого значення нова науково-технічна дисципліна – телематика, предметом якої є методи передачі інформації на відстані, які значно перевищують лінійні розміри площі, які зайняті учасниками звязку. Телематика – це ще й назва безпаперової технології, яка виключає використання носіїв інформації на проміжній стадії її обробки. Отже, на поверхні питання максимального набліження рівнів гуманітарних і технічних знань, їх подальшої інтеграції. На умовах такого підходу в питаннях дослідження бізнес-процесів, побудованих на засадах сучасних телекомунікаційних систем і технологій їх результати будуть мати сучасний характер і перспективу свого подальшого розвитку.

Саудівський богослов видав фетву, у якій засудив використання Wi-Fi іншої людину без дозволу. «Користуватися Wi-Fi нелегально або без відома бенефіціаріїв або постачальників послуг неприпустимо, — говориться у фетві, випущеної Алі аль-хакамі, членом Верховного комітету з наукових досліджень і релігійному праву Саудівської Аравії. — Необхідно консультуватися з постачальником послуги або людиною, що платять за неї гроші, перш ніж її використовувати». Особливо уточнюється, що немає гріха в тому, щоб використовувати загальнодоступний Wi-Fi у парках, торгових центрах, готелях, кафі й урядових закладах. (***Фетва*** *— рішення по суспільному, політичному або правовому питанню, що виноситься високопоставленим ісламським богословом — муджтахидом*).

Питання безпеки ніколи не втрачають актуальності. Їхньому вивченню присвячена безліч фундаментальних досліджень, сотні монографій, написане тисячі статей. Традиційно питання розглядається через тріаду: безпека держави – безпека регіону – безпека підприємства. Це зрозуміло й логічно. По-перше, легко з'ясовна логіка класичної ієрархії. Міняється тільки напрямок, залежно від завдань дослідження цього питання: від безпеки держави до безпеки підприємства або навпаки. Це різні аспекти розгляду. А тому включаються різні механізми переходу від одного рівня безпеки до іншого. Й, природно, взаємозв'язок, взаємозалежність і взаємозумовленість об'єктивних і суб'єктивних факторів.

Основною першопричиною появи погрози безпеки можна назвати, спираючись на роботи відомих авторів, порушення рівноваги. Найрізноманітнішої рівноваги, практично у всіх сферах життєдіяльності окремої людину, колективу, суспільства, держави. Рівноваги економічного, екологічного, енергетичного, демографічного, технологічного, фізіологічного, споживчого, продуктивного, майнового характеру тощо.

Технології, методи й способи забезпечення безпеки можуть бути найрізноманітнішими. Це залежить від того, у який сфер життєдіяльності виникла погроза. Можна, наприклад, закрити кордони. Організувати тотальний контроль і встановити відповідний режим. Створити спільну систему безпеки. Розробити й впровадити

високотехнологічні системи захисту. Увести строго регламентовану систему розподілу ресурсів. Заборонити певні види діяльності. І багато інших способів і методів забезпечення безпеки.

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 погроза як фактор може й не з'явитися! Навіщо ж витрачати час і гроші на їхні попередження. З'явиться погроза, будемо усувати. Інший підхід полягає в тому, щоб завчасно направити зусилля на виявлення потенційних погроз і створення ефективних механізмів їх усунення.

І перший і другий підходи цілком з'ясовні. Перший, потрібно це визнати, більше пов'язаний з ризиком втрат, як для підприємства, так і для регіону або країни в цілому. Але, якщо все буде організовано грамотно, професійно й керівництво буде далекоглядним, тобто ймовірність того, що умови для виникнення погроз будуть зведені до мінімуму. Будуть зекономлені ресурси. Ну а якщо погроза виникне, природно доведеться витратитися й передбачити можливість повторення, закріпівши придбаний досвід.

Але ситуація може складатися по-різному, обставини, під впливом як внутрішніх, так і зовнішніх факторів (несприятливих, природно) 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.

Із цього можна зробити висновок, що платформою для прийняття рішень є фактор економічної безпеки. Прийнято розрізняти три рівні безпеки:

- національний (міжнародний);
- мезоэкономический (регіональний);
- мікроекономічний (рівень підприємств і індивідів).

Для характеристики економічної безпеки підприємства найчастіше використовуються показники фінансового становища й результатів його господарської діяльності. Тобто, використовується старий інструментарій, а нові поняття не вводяться. Так само, як і не вводяться нові поняття цієї категорії. Найпоширенішим визначенням економічної безпеки підприємства ототожнюється стан його захищеності від негативного впливу на нього зовнішніх і внутрішніх факторів (погроз), 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, у першу чергу, 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.

Ознаками порушення економічної безпеки на підприємстві в першу чергу 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 і т.д. Усе більше й більше привертає увагу питання безпеки для підприємств телекомунікаційної галузі. Причина зрозуміла - усі сучасні бізнес-процеси реалізуються на основі телекомунікаційних систем і технологій, стрімко розвивається електронна комерція.

Наприклад, компанія Alibaba є найбільшою платформою для оптової торгівлі. Мільйони покупців і продавців із усього світу є її клієнтами. Використовуючи сучасні телекомунікаційні системи й технології, компанія дає постачальникам можливість зв'язатися з покупцями із усього світу, а покупцям - зручні інструменти пошуку товарів і партнерів для бізнесу. Масштаби колосальні: у каталозі більш 400 мільйонів товарів, покупці й продавці більш ніж з 190 країн миру. Асортимент товару - від промислового встаткування 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 комерции, постійно розвивається технологічно, залучає для розвитку бізнесу самі останні досягнення в області 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 області телекомунікацій. Але погрози для безпеки підприємства й, в остаточному підсумку, для його клієнтів, починають формуватися з рівня примітивного шахрайства, досягаючи у своєму розвитку вдосконалюванні технологічних вершин.

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 коштів, 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.

Суть послуги, наданої телекомунікаційним підприємством, полягає в переміщенні програмного продукту споживачеві. Що може відбутися на цій лінії діяльності підприємства? Можуть виникнути проблеми, зв'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, послугами якої користується телекомунікаційне підприємство.

Найбільш очевидною погрозою для телекомунікаційного підприємства є нелегальне або, що буде точніше, несанкціоноване використання трафіка. Іншими словами, саме звичайне злодійство. Причому, технологія злодійства й подальшого незаконного використання трафіка не стоїть на місці, а поступово розвивається. І розвивається паралельно розвитку телекомунікаційних систем і технологій. Найпоширенішим є використання GSM-шлюзів.

GSM-шлюз дозволяє переводити телефонний трафік з мереж стандартних у мережі мобільного зв'язку цього ж стандарту, GSM. І, як правило, використовується для скорочення видатків на корпоративний зв'язок у компанії. Головна відмінність даного пристрою від звичайного мобільного телефону – це многоканальность. Тобто, на кожний канал може підключатися сім-карта певного оператора.

Як у цьому випадку працює підприємство? Існує спеціальна програма, у якій накопичується інформація про зроблену послугу зв'язку. Далі накопичена інформація надходить в іншу програму, яка здійснює облік взаємних витрат підприємства й споживача на зроблену послугу – биллинг. Можуть бути й інші алгоритми. В остаточному підсумку послуга проходить тарифікацію, дані надходять у відповідні підрозділи підприємства, у бухгалтерію, зокрема.

Саме на це не можна не звертати уваги, у плані оцінки можливої економічної небезпеки для підприємства. Якщо в ланцюжок діяльності підприємства по наданню послуги зв'язку вбудовано кілька програм, то зрозуміло, що чим більше таких програм, тем вище ризик можливих втрат через викривлення окремих параметрів переданої інформації. І це, у першу чергу, питання внутрішньої економічної безпеки, тому що така інформація доступна тільки співробітникам компанії. Так наприклад, руководитель однієї з фирм завдав Белтелекому збитків на 2,8 миліарди карбованців, заробляючи на незаконних послугах. Діючи в порушення виключного права національного оператора зв'язку, шахрай, використовуючі спеціальне устаткування, призначене здійснювати перетворення телефонного сигналу, виступили в ролі посередника по доставці міжнародного трафіка. Ограбував національного оператора. Протягом півроку незаконно одержав дохід у сумі

більш 40 тисяч доларів. Приклад звичайного шахрайства на телекомунікаційнім підприємстві.

Розвивається телекомунікаційна галузь і не відстає в розвитку телекомунікаційне шахрайство (більш 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 джерелах втрати від несанкціонованого доступу до послуг зв'язку становить у середньому 5 % від доходів. Що 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 й навряд чи це буде приваблювати клієнтів). По-третє, це дає можливість шахрая оцінити ефективність своєї роботи й удосконалювати методи.

Висновки. Проблема шахрайства в кіберпросторі має світовий статус, оскільки представляє ідеологію «злодіїв у законі», що прагнуть жити за рахунок інших. Одним з основоположних принципів міжнародного права, та й національних систем права є справедливість, який рівною мірою є важливим і цінним і у всіх сферах життєдіяльності суспільства й держави та повинен неухильно дотримуватися щоб уникнути порушення рівноваги, як фактору економічної безпеки. Одним з напрямів утримання балансу в сфері економічної безпеки підприємств телекомунікаційної галузі є максимальне набліження рівнів гуманітарного й технічного знання як науковців, так і практиків.

Литература

1. *Гапоненко В.Ф. Экономическая безопасность предприятий. Подходы и принципы/ Беспалько А.Л., Власков А.С. – М.: Издательство «Ось-89», 2007. – 208 с.*
2. *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.*
3. *Дашян М. С. Право информационных магистралей (Law of information highways)//Вопросы правового регулирования в сфере Интернет, — М: "Волтерс Клувер", 2007.*
4. *Джабраилов И. Мобильная связь: конкуренция и тенедниции развития // Телекоммуникации. – 2005. - №02(002). – С. 7-10.*
5. *Кириллов И. Мировой рынок СХД: очередной год развития // Сети &Бизнес. – 2015.- №1(80). - С. 31-35.*
6. *Кириллов И. Украинский рынок ИТ: жизнь после революции // Сети &Бизнес. – 2014.- №1(74). - С. 14-20.*
7. *Новикова І.В. Управління конкурентоспроможністю телекомунікаційних підприємств: теорія, методологія, практика: монографія / И.В. Новикова. – Миколаїв: ФОП Швец В.Д., 2013. – 296 с.*
8. *Преступления в сфере информационных технологий [Электронный ресурс]. — Режим доступа: http://ru.wikipedia.org/wiki*
9. *Феофилова Т.Ю. Методология исследования экономической безопасности региона // Современные проблемы науки и образования. – 2014. – № 4.;URL: [Электронный ресурс]. — Режим доступа: http://science-education.ru/ru/article/view?id=14216 (дата обращения: 20.06.2016).*

Гудзь Елена Евгеньевна, Сотниченко Владимир Николаевич. Экономическая безопасность телекоммуникационных предприятий: проявления угроз и их избегания. *В статье рассматриваются вопрос возникновения угроз для экономической деятельности*

телекоммуникационных предприятий. Рассматриваются причины и признаки появления угроз, механизмы их реализации, способы незаконного использования трафика оператора.

***Ключевые слова**: экономическая безопасность, угроза безопасности, мошенничество, проявления коррупции, права национального оператора.*

***Gudz Olena, Sotnychenko Volodymyr. Economic security of telecommunication enterprises: symptoms of threats and their avoidance.** In the article examined question of origin of threats for economic activity of telecommunication enterprises. Reasons and signs of appearance of threats, mechanisms of their realization, methods of the illegal use of traffic of operator are examined.*

***Keywords**: economic security, threat safety, swindle, displays of corruption, rights for a national operator.*

УДК 330.341

Каїра З.С., д.е.н., проф.,
Донбаська державна машинобудівна академія
Ващенко О.П., д.т.н.,проф.,
Державний університет телекомунікацій

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ МАЛИХ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ

Узагальнено основні передумови економічного розвитку малих телекомунікаційних підприємств. Досліджено зарубіжний досвід підтримки нових підприємств у високотехнологічних галузях. Охарактеризовано особливості функціонування малих підприємств у стратегічних альянсах. Виокремлено потенційні вигоди основних стейкхолдерів від інтенсивного розвитку малих телекомунікаційних підприємств. Визначено необхідність інтенсивного використання інформаційно-комунікаційних технологій підприємствами малого бізнесу, охарактеризовано особливості стратегічних альянсів та аутсорсингу телекомунікаційних послуг. Розроблено прогноз розвитку показника кількості малих телекомунікаційних підприємств України.

***Ключові слова**: телекомунікаційне підприємство, малий бізнес, стратегічний альянс, аутсорсинг, глобальні ланцюги постачання телекомунікаційних послуг, прогноз, прибуток.*

Постановка проблеми. Телекомунікації є ключовим чинником в усіх сферах діяльності суспільства, забезпечуючи підтримку розвитку економіки держави. Інтенсивне використання компаніями інформаційно-комунікаційних технологій (ІСТ) є передумовою успіху підприємств у інноваціях, конкурентоспроможності та економічному зростанні. У той час, коли великі компанії намагаються використовувати переваги, що пропонуються інформаційно-комунікаційними технологіями, малі телекомунікаційні підприємства мають пристосовуватися до сучасних вимог, інакше ризикуючи залишити цифрові ланцюги постачання телекомунікаційних послуг. Зважаючи на велику різноманітність видів малого підприємництва, нагальною проблемою є виокремлення перспектив та умов економічного зростання для малих телекомунікаційних підприємств, що мають вагомий потенціал у прискоренні темпів зростання науково-технічного прогресу країни. Рішення цієї проблеми потребує аналізу стану малих телекомунікаційних підприємств Україні, визначенні перспектив та вигід від економічного розвитку цього показника.