УДК 338.246.8

Сучасні виклики та тенденції економічної безпеки телекомунікаційних підприємств

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

У статті розглядаються питання передумов виникнення загроз для економічної безпеки. Визначаються характер загроз, ознаки і джерела їх виникнення. Вказано на основні передумови виникнення загроз і шляхи їх подолання. На прикладі телекомунікаційних підприємств показано практичні наслідки впливу загроз. Наголошено на необхідності законодавчого врегулювання питань взаємодії телекомунікацій та інфраструктури.

Ключові слова: виклик-відповідь, економічна безпека, телекомунікаційне підприємство, джерело загроз, класифікація загроз, кібератаки.

Сотниченко В.Н. СОВРЕМЕННЫЕ ВЫЗОВЫ И ТЕНДЕНЦИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ ПРЕДПРИЯТИЙ

В статье рассматриваются вопросы предпосылок возникновения угроз для экономической безопасности. Уточняются характер угроз, признаки и источники их возникновения. Указано на основные предпосылки появления угроз и пути их преодоления. На примере телекоммуникационных предприятий показаны практические последствия влияния угроз. Сделан акцент на необходимости законодательного урегулирования вопросов взаимодействия телекоммуникаций и инфраструктуры.

Ключевые слова: вызов-ответ, экономическая безопасность, телекоммуникационное предприятие, источник угроз, классификация угроз, кибератаки.

Sotnychenko V.M. MODERN CHALLENGES AND ECONOMIC SECURITY TRENDS TELECOMMUNICATIONS COMPANIES

The article discusses the causes of threats to economic security. Clarifies the nature of the threats, the signs and the sources of their origin. Indicated on the underlying causes and conditions for the appearance of threats and ways to overcome them. For example, telecommunications companies are shown the consequences of threats to their future work. The necessity of legislative regulation of the issues of interaction of telecommunications and infrastructure.

Keywords: challenge-response, economic security, telecommunications company, source of the threats, classification of threats, cyber attacks.

Постановка проблеми у загальному вигляді. Безпека як категорія, що визначає стан перебування будь-якого об'єкта в реальній дійсності, має кілька аспектів. Наявність багатоаспектного підходу до розглядання категорії «безпека» зумовлена перш за все походженням самого об'єкта (джерелом виникнення), природою суб'єкта, характером і видом його діяльності.

Все, що існує в об'єктивній реальності, існує з необхідністю. Існування кожного об'єкта обумовлено певними потребами його появи. Залежно від потреб об'єкт від початку своєї появи наділений функціональним апаратом, який активізується тоді, коли складаються конкретні умови.

Насамперед необхідно уточнити поняття «проблема». Проблема – це категорія, яка виникає в рамках процесу людської діяльності, тобто має суто суб'єктивну природу. Проблему створює людина. Передумови виникнення проблеми теж мають суб'єктивний характер. Треба розрізняти поняття «проблема» и «труднощі». Труднощі – це закономірні наслідки проблеми. Й проблема, й труднощі – це «виклик». Тільки відповіді різні. Труднощі долаються шляхом застосування додаткових ресурсів системи, проблема – шляхом зміни системи, її перебудови. Це важливо, оскільки, якщо буде неправильно класифіковано виклик (проблема чи труднощі), неадекватними будуть і прийняте рішення, і результати його реалізації. Для економічної безпеки телекомунікаційного підприємства, де всі операції щодо управління бізнесом на технологічному рівні відбуваються за долі секунди, це реальна загроза.

Аналіз останніх досліджень і публікацій. За джерелом виникнення об'єкти умовно можна поділити на природні та позитивні (продукт людської діяльності). Що стосується природних джерел, то вони мають географіч-

ний та кліматичний характер: клімат, ландшафт, надра, гідросфера, екосистеми тощо. Решту можна віднести до продуктів людської діяльності, що з'являються за ступенем появи тих чи інших людських потреб. Поява певних людських потреб обумовлена багатьма чинниками, але механізм їх появи формується у процесі еволюції (на глобальному рівні) і у процесі змін звичних умов життєдіяльності (на більш прагматичному рівні).

Будь-які зміни є сигналом про початок порушення стабільності встановленого порядку речей та стійкості екосистеми. Це сигнал до того, що починається період наростання небезпеки, тому необхідно вибудовувати систему захисту. В контексті нашої статті це є центральним предметом уваги. Економічна безпека взагалі не може бути гарантованою на 100%, але максимально підняти цей показник можна. Про це далі.

Без розуміння названих вихідних постулатів щодо безпеки неможливо побудувати цілісну картину і адекватну систему поглядів на цю проблему. На платформі цілісного бачення проблеми безпеки буде неважко розібратися і з економічною безпекою, і з екологічною, і з особистою, і з будь-якою іншою. А з огляду на домінуючу сьогодні світоглядну картину матеріальності світу економічна безпека також є домінуючої для людського суспільства в будь-яких формах його організації. Цьому питанню присвячено чимало досліджень, серед авторів яких слід назвати Л.І. Абалкіна, Є.Д. Кормишкіна, І.М. Петренка, які розглядали економічну безпеку як сукупність умов і факторів, що забезпечують стійкість національної економіки. Є.Є. Гутман, В.К. Сенчагов, О.О. Пороховський робили акцент на такому стані економіки, який здатний захистити її життєво важливі інтереси. М.М. Блінов, Г.В. Коржов, В.І. Митрохин у своїх працях доводили, що економічна безпека є предметом піклування держави. Різниця в судженнях і підходах простежується і в працях таких дослідників питань економічної безпеки, як, зокрема, О.Л. Пластун, Н.В. Ващенко, С.О. Дмитров, В.Є. Духов,Т.А. Медвідь, І.П. Мігус, Л.М. Сумець, М.Б. Тумар, Л.І. Донець, Л.М. Художлій, С.М. Побережний, М.І. Зубок. Але при цьому слід зазначити, що незалежно від розбіжностей у підходах і поглядах результати досліджень названих авторів складаються в картину цілісного і відносно повного бачення проблеми.

Виділення не вирішених раніше частин загальної проблеми. Магістральною метою життєдіяльності людини, суспільства і держави є забезпечення свого існування на рівні задоволення, перш за все задоволення потреб на фізіологічному рівні, на рівні матеріальному. Це є базою для подальшого всебічного розвитку – інтелектуального, розумового, духовного.

Спокій і стабільність є характерними і головними ознаками безпечного стану, але це зовсім не означає, що в ідеалі так повинно бути постійно. Так буває лише тоді, коли немає розвитку, прогресу, руху вперед. Якщо все стабільно, рівно і спокійно, то це перший сигнал до того, що вже виникла реальна загроза і треба вживати запобіжних заходів, щоб уникнути втрат [2, с. 4].

Ілюстрацією такого твердження може бути розпад Радянського Союзу, якому передував затяжний період застою (стагнації). В цей фатальний для радянської системи період до її керівного центру надходили тривожні сигнали за всім спектром напрямів її функціонування: початок процесів системної дезінтеграції, зниження темпів зростання виробництва, скорочення товарообігу на зовнішньому ринку, конфлікти на міжнаціональному ґрунті тощо [8, с. 34].

Ці тривожні сигнали є не чим іншим, як викликами до самої системи, попередженнями про те, що наближається її крах. Виклики логічно вказували на необхідність адекватних відповідей. Англійський історик і філософ Арнольд Тойнбі вивів ***«закон виклику та відповіді»***, який, на його думку, є визначним у розвитку цивілізації [1, с. 86]. Тобто певна ситуація або, скажімо, чинники ставлять перед суспільством запитання (*«виклик»*), на яке треба реагувати. Подальша доля суспільства буде залежати від відповіді, яку воно дасть, якою воно відреагує на виклик. Відповіді (реагування) можуть бути різними через різні причини. Наприклад, низький професіоналізм і некомпетентність керівництва, брак або ж повна відсутність необхідних ресурсів, невірна оцінка рівня загрози і, що не менш важливо, рівень технологічного забезпечення тощо.

А. Тойнбі вважав, що проблему виклику може успішно вирішити лише адекватна відповідь, тобто проблему як загрозу усунути і вивести суспільство на новий рівень розвитку. Генерувати таку відповідь може активна меншість, тобто керівництво на своїх рівнях відповідальності, а саме керівництво компанії, підприємства, будь-якої форми суспільної організації. Воно не тільки виробляє адекватне рішення, але й створює механізм його реалізації на умовах довіри серед колективу і його готовності підтримати своє керівництво.

Важливим фактором, який керівник не може ігнорувати, є те, що вибір варіантів є

вільним, незумовленим. А відповідальність за наслідки прийнятого рішення є персональною. Це закон.

Формулювання цілей статті (постановка завдання). На думку автора, важливими завданнями в контексті статті є:

– конкретизація та впорядкування викликів (загроз) і змін, які вони за собою логічно тягнуть в галузі економічної безпеки з урахуванням особливостей функціонування телекомунікаційного підприємства;

– характеристика та оцінка діючих моделей протидії загрозам економічної безпеки;

– ілюстрація дії наведених моделей на конкретних прикладах.

Виклад основного матеріалу дослідження. До викликів як передумов змін, котрі порушують спокій і стабільність, можна віднести такі фактори:

– вдосконалення, оптимізація, урізноманітнення суспільних форм взаємовідносин в процесі життєдіяльності;

– технічний прогрес, а також запровадження його результатів у практику життя;

– збільшення обсягу інформації, доступної широкому колу користувачів;

– технологічні виклики;

– розширення меж світоглядних інтересів;

– поява нових потреб;

– обмеження ринків збуту товарів і послуг;

– природні та техногенні катастрофи;

– світові або локальні конфлікти тощо.

Викликів, які закономірно потребують адекватного реагування, насправді значно більше. Кожен виклик приводить до відповідних змін, створює нові умови, за яких визрівають і формуються нові виклики [10, с. 11; 7, с. 33–38]. І так нескінченно. А наведений перелік має суто орієнтуючий характер.

Щодо результатів, які формуються під впливом змін, то вони, наприклад, можуть бути такими:

– поява нових форм спілкування;

– формування нових комунікативних систем і технологій;

– ревізія форм організації ділової взаємодії, а також вихід на новий рівень;

– оновлення методів діагностики та профілактики;

– початок пошуку нових технологічних рішень.

Формується нова життєздатна модель організації взаємодії на всіх рівнях життєдіяльності людини, суспільства і держави. Саме цей період є найбільш небезпечним, з'являються загрози, які здатні реально руйнувати форми організації взаємодії, комунікативні канали, інформаційні системи [4, с. 110–114].

Загрози примушують систему змінюватися у напрямі створення нової моделі, здатної протистояти загрозам, нейтралізувати їх. Підходи щодо створення оновленої моделі продуктивної взаємодії в суспільстві можуть бути різними.

Перший варіант, і він є більш традиційним, полягає в оперативному реагуванні на загрози з метою їх знищення. При цьому система (компанія, підприємство) не припиняє своєї діяльності. На тих напрямах її діяльності, які найбільше піддаються деструктивному впливу загроз, максимально концентруються всі можливі ресурси, і починається процес «лікування» («латання дірок»).

Очевидно, що зосередження ресурсів на одному напрямі послаблює позиції на інших. Зменшується продуктивність підприємницької діяльності, що позначається та темпах виробництва, якості товарів або послуг та їх собівартості, конкурентоздатності тощо. З'являються класичні ознаки початку кризи [9].

Питання, що постають перед керівництвом підприємства, можна звести приблизно в такі групи:

– ***перша:*** якими є масштаби загрози;

– ***друга:*** як можна зберегти, а за можливості й покращити фінансові потоки;

– ***третя:*** до якого сценарію треба бути готовим;

– ***четверта:*** як реагувати на стратегічні зміни.

Якщо конкретизувати питання, що входять до цих умовних груп, то керівництво поволі ставить для себе питання і такого характеру: яких заходів треба вжити; чим моя ситуація краще або гірше інших; наскільки стабільним є моє фінансове становище; діяти чи зачекати; як прискорити прийняття рішень.

Цей період, коли йде інтенсивний пошук варіантів вирішення проблеми, коли починаються реконструкторські роботи на рівні бізнес-моделей, є найбільш ризикованим для економічної безпеки компанії. Наприклад, це можна пояснити тим, що перебудова системи функціонування підприємства закономірно супроводжується послабленням зв'язку між її складовими елементами: між виробництвом і ринком, між ціною і якістю, між попитом і пропозицією тощо [3; 11, с. 22].

Ці слабкі місця і використовуються носіями загроз для досягнення своїх цілей. При цьому варіанті боротьби із загрозами компанія продовжує працювати, намагаючись збе-

регти свої позиції в бізнесі. Прикладом може служити хакерська атака на компанію «Київстар», крупного оператора мобільного зв'язку в Україні.

Згідно з повідомленням інформаційного агентства «ЛІГА Бізнес Інформ» в серпні 2016 року на мережі мобільного оператора, за версією керівництва компанії, здійснено IP-атаки такого рівня, яких в Україні до цього не було. Сегмент ринку, забезпечуваний компанією, почав давати збої: послуги голосових дзвінків і передачі даних в Києві працювали нестабільно. На думку фахівців компанії, це пов'язано з повною заміною в Києві телекомунікаційного обладнання швецької фірми "Ericsson" на обладнання від "Huawei". Заміна, оновлення, модернізація чи оптимізація системи загалом або ж її елементів створюють прецедент для здійснення атак. Саме в цей час відбувається певний перерозподіл ресурсу і за цих обставин ймовірним може бути поява слабких місць в системі, які ретельно відшукуються і потім використовуються атакерами.

Як відомо, мобільний зв'язок вже відносно давно і активно використовує Інтернет. Саме цим каналом і могла бути здійснена IP-атака. Працівники компанії і раніше відзначали спроби атак, але вони були невдалими, оскільки мережа «Київстар» побудована за сегментним принципом, що означає, що, коли не витримує один сегмент, навантаження перерозподіляється на інший. Це стосується каналу голосового мобільного зв'язку. Але у цьому випадку ситуація набагато складніша, оскільки атака була здійснена на Інтернет, канал передачі даних.

Аналогічна атака в жовтні 2016 року була здійснена на російського мобільного оператора «Мотив». В результаті атаки у користувачів припинив працювати не лише голосовий зв'язок, але й мобільний Інтернет. «Мотив» надає послуги зв'язку з 1996 року і є крупним оператором в РФ. У 2014 році оператор запустив підтримку мереж 4G, а потім і взагалі зробив безкоштовними голосовий зв'язок і текстові повідомлення. Тільки серйозні компанії із солідним капіталом можуть піти на такий крок. І саме вони є найбільш привабливими об'єктами для атак.

Економічна безпека телекомунікаційного підприємства (оператора зв'язку) сама по собі не представляє повної картини катастрофічних наслідків потенційних загроз, якщо розглядати її у відриві від інфраструктури. Доступ до інфраструктури з метою надання інфокомунікаційних послуг – це те, на чому заробляють свій капітал телекомунікаційні компанії. Тому питання врегулювання на законодавчому рівні відносин, пов'язаних зі встановленням єдиних правових засад доступу та використання інфраструктури, є в Україні одним із найактуальніших.

Економічна безпека підприємств суміжних галузей безпосередньо залежить від здатності телекомунікаційних підприємств протистояти спробам втручатися в їх бізнес-процеси.

Епоха зломів банківських сейфів і сховищ вже практично в минулому. Обслуговування цього специфічного сегменту інфраструктури є найбільш важливим для телекомунікаційних компаній. Так, згідно з даними «Лабораторії Касперського» в листопаді 2016 року на сервери п'яти російських банків було здійснено серію хакерських атак. Це було підтверджено в прес-службах «Ощадбанку» і «Альфа-банку».

DDoS-атаки було організовано з ботнетів десятків тисяч машин, територіально розташованих в десятках країн, і тривали протягом двох діб. Згідно з повідомленням агентства «РИА Новости» більше половини атак було здійснено з території США, Індії, Тайваню та Ізраїлю. Всього в атаках брали участь машини з 30 країн. Для того щоб уявити реальну небезпеку таких атак, слід звернути увагу на технологічний аспект проблеми: середня тривалість кожної атаки становила близько години, найдовша за часом тривала майже 12 годин. І, увага, потужність атак досягала 660 тисяч запитів на секунду. Однак системи захисту банків відпрацювали надійно, атаки були своєчасно виявлені і локалізовані підрозділами кіберзахисту.

Це конкретний приклад роботи телекомунікаційного підприємства у напрямі захисту від втручання у сферу економічних інтересів. Клієнтура банків не тільки не постраждала від цих атак, але й не помітила їх. Слід відзначити, що це були складні атаки, котрі практично неможливо відбити стандартними засобами захисту, якими користуються оператори зв'язку.

Висновки з цього дослідження. Отже, щодо сучасних викликів та тенденцій економічної безпеки телекомунікаційних підприємств можна зробити такі висновки:

– всі дії в напрямі втручання в життєвий простір інших структур, об'єктів, систем, людей обумовлені закономірно: відбуваються порушення певних пропорцій, умов, форм організації взаємодії, векторів життєвих інтересів, що послаблює здатність протистояти загрозам економічній безпеці;

– сьогодні є два підходи до боротьби із втручанням в економічну безпеку телекомунікаційних підприємств: створення комплексу оперативного реагування на загрози по факту їх виникнення і створення резервної моделі виробництва, яка включається замість основної у разі її пошкодження (на прикладі сегментної мережі «Київстару»);

– слабким щодо протистояння загрозам для підприємств телекомунікації є зв'язок з інфраструктурою, який сьогодні в Україні недостатньо врегульований на законодавчому рівні;

– прямою і зростаючою загрозою для економічної безпеки телекомунікаційних підприємств є хакерські атаки, через які стаються великі економічні втрати.

Наведені у висновках позиції є перспективними щодо їх дослідження на науково-практичному рівні. Вони повинні розглядатися в комплексі й у взаємозв'язку як взаємообумовлені. Але якщо створення систем захисту від загроз має більш технологічний характер, то питання законодавчого врегулювання взаємодій підприємств телекомунікації з інфраструктурою є пріоритетним завданням держави.

ЛІТЕРАТУРА:

1. Тойнби А.Дж. Постижение истории / А.Дж. Тойнби. – М.: Айрис-Пресс, 2002. – 640 с.
2. Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение / Л.И. Абалкин // Вопросы экономики. – 1994. – № 12. – С. 4.
3. Блинов Н.М. Экономическая безопасность центра и регионов / Н.М. Блинов // Общественные науки. – 1996. – № 2. – С. 33.
4. Буркальцева Д.Д. Модель взаємодії векторів розвитку та загроз економічній безпеці / Д.Д. Буркальцева // Формування ринкових відносин в Україні. – 2012. – № 9 (136). – С. 110–114.
5. Гончаренко Л.П. Процесс обеспечения экономической безопасности предприятия / Л.П. Гончаренко // Справочник экономиста. – 2005. – № 2. – С. 14–18.
6. Гончаренко Л.П. Процесс обеспечения экономической безопасности предприятия / Л.П. Гончаренко // Справочник экономиста. – 2005. – № 3. – С. 14–19.
7. Забродский В.В. Теоретические основы экономической безопасности отрасли и фирмы / В.В. Забродський, Н.П. Капустин // Бизнес-Информ. – 2008. – № 15–16. – С. 33–38.
8. Пастернак-Таранушенко Г.В. Экономическая безопасность государства: [учебник для государственных служащих] / Г.В. Пастернак-Таранушенко; под ред. Б.Н. Кравченко. – К.: Институт государственного управления и самоуправления при Кабинете Министров Украины, 1994. – 140 с.
9. Пороховский А.А. Россия и современный мир / А.А. Пороховский // Вопросы экономики. – 1995. – № 1. – С. 128.
10. Сенчагов В.К. Экономическая безопасность / В.К. Сенчагов // Производство. Финансы. Банки. – М.: ЗАО «Финстатинформ», 1998. – С. 11.
11. Сенчагов В.К. Экономическая безопасность России: [учебник] / В.К. Сенчагов. – М.: Дело, 2005. – С. 22.