умовою успіху компанії на міжнародному ринку, тому для прийняття правильних управлінських рішень у сфері міжнародного маркетингу компаніям необхідно створювати маркетингові інформаційні системи.

1. *Азарян Е.М.* Международный маркетинг. – К., 1998. 2. *Багиев Г.Л., Моисеева Н.К., Никифорова С.В.* Международный маркетинг. – С.Пб., 2001. 3. *Білорус О.Г., Лук'яненко Д.Г.* Глобалізація і безпека розвитку. – К., 2001. 4. *Ванифатова М.М.* Системы маркетинговой информации: современные мировые тенденции развития и особенности российского рынка // Маркетинг в России и за рубежом. – 2002. – № 1 // www.cfin.ru/press/marketing. 5. *Пелішенко В.П.* Маркетинговий менеджмент: Навч. посібник. – К., 2003. 6. *Старостіна А.О.* Маркетингові дослідження. Практичний аспект. – С.Пб., 1998. 7. *Kotler P.* Marketing Management: Analysis, Planning, Implementation. – 9th ed. – N.J., 1997.

Надійшла до редколегії 30.03.04

О.І.Ступницький, канд. екон. наук, доц.

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ГЛОБАЛІЗАЦІЇ: СФЕРИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

Розглянуто інформаційну безпеку як важливу складову прискореного розвитку інформаційних технологій та формування глобальних світових інформаційних мереж.

An accelerated development of IT and establishment of the world information networks and integration of Ukraine into the world information community are revealed.

Сучасний міжнародний бізнес неможливо уявити без інформаційних технологій. Відомо, що понад 70 % світового сукупного національного продукту залежить тим чи іншим чином від інформації, що зберігається в інформаційних системах. Глобалізація комп'ютерних мереж створила не тільки відомі зручності та переваги, але й проблеми. Однією з найбільш важливих сьогодні є проблема інформаційної безпеки.

Дослідження останніх років, що проводяться спеціалізованими фірмами США, Великої Британії та інших країн, щорічно виявляють десятки тисяч випадків порушення інформаційної безпеки. Це не стільки прямі крадіжки, вандалізм та, у зв'язку з цим, прямі втрати даних ПК фірм, скільки зовнішнє підключення до комп'ютерної мережі компанії, використання доступу до інформаційних систем компаній самих робітників компаній та їх трансфертні операції грошей на приватні банківські рахунки, цільові програми "вірусних нападів", а також прості людські помилки операторів при використанні програм у позаконтурних комп'ютерних системах. Загальні суми втрат компаній сягають сотень мільйонів доларів. Це, безумовно, свідчить про гостру актуальність проблеми інформаційної безпеки для всіх без винятку суб'єктів сучасного світового ринку.

Для оцінки та розробки стандарту інформаційної безпеки перш за все постає завдання забезпечення державних та комерційних організацій інструментом для створення її ефективних систем на основі сучасних методів менеджменту, а саме: методу моделювання процесів та оцінки ефективності; методу декомпозиції та структуризації компонентів; методу оцінки ефективності функціонування та прийняття рішень.

Власне політика інформаційної безпеки являє собою суму правил, що регулюють використання інформації, її обробку, розподіл та представлення у продукті чи системі.

У 1998 р. Британський Інститут Стандартів (BSI) за підтримки комерційних організацій, серед яких були Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica та інші, розробив та впровадив стандарт інформаційної безпеки BS7799. Він став узагальненням дійсно найпередовіших досягнень в організації інформаційної безпеки підприємства чи організації.

На сьогоднішній день стандарт BS7799 визначає загальну організацію, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику тощо в контексті інформаційної безпеки. Основна мета – скоротити матеріальні втрати, пов'язані з порушенням інформаційної безпеки. Важливим є те, що стандарт, перш за все, призначений для економії фінансових витрат фірм, а в деяких випадках навіть перешкоджанню банкрутства, а не є зовнішньою обов'язковою вимогою, що призводить до додаткової статті витрат фірм.

Стандарт BS7799 – це модель системи менеджменту, і в цьому сенсі не є технічним стандартом, до нього не надається тих чи інших відповідних алгоритмів кодування, окрім вимоги "Особливо важлива інформація повинна бути закодована". Сама фірма, базуючись на загальних принципах застосування стандарту, вирішує, яка інформація є для неї важливою і у який спосіб необхідно провести її кодування. Офіційні Рекомендації щодо застосування стандарту є гнучкими залежно від сфери бізнесу: торгівля, банківська та страхова справа тощо. Такий підхід до інформаційної безпеки на основі мети та завдань менеджменту, а не фіксованих технічних специфікацій, є принциповим для стандарту BS7799 як стандарту системи управління.

Сьогодні в Україні більша частина спеціалістів по інформаційній безпеці займаються, в основному, технічними аспектами захисту даних, причому для багатьох з них – це криптографія. Це, безумовно, вплив "радянського" періоду, коли в нашій країні захист інформації був прерогативою військових відомств та спецслужб, коли основною метою було забезпечення максимальної конфіденційності. Тому створений у результаті цього "дисбаланс технічних засобів" не відповідає нинішнім критеріям ефективного функціонування на ринку. Перед комерційними та державними господарськими структурами сьогодні стоїть більш важливе завдання: не тільки забезпечити надійний захист інформації, але й організувати ефективний доступ до даних і роботу з ними. Саме ця ідея лежить в основі стандарту BS7799.

Вимоги до гарантій відокремлені від вимог функціональності.

Групування послуг з безпеки інформації (відповідно до загальних або специфічних завдань безпеки) відбувається за класами послуг (градація: реальна стійкість, реальні функціональні можливості, вибірковість дій). При цьому вектор реалізації кожної послуги залежить від форм загроз певного класу.

При розробці критеріїв в основу були покладені такі принципи: всі аспекти проблем безпеки інформації не повинні бути прив'язані до тої чи іншої політики безпеки; можливості виміру узгодженості послуг щодо стійкості, функціональних можливостей та вибірковості дій; відповідність кожної послуги у сфері захисту інформації конкретним існуючим або потенціальним загрозам, що можуть виникнути при використанні комп'ютерних систем.

Відомо ще з математичної статистики, що ризик визначається як множник можливої втрати та можливості, що ця втрата відбудеться. Під втратами ми розуміємо матеріальні втрати, пов'язані з порушенням наступних властивостей інформаційного ресурсу: конфіденцій-

ність, цілісність, доступність, нагляд (управління доступом). Важливо, що стандарт не забезпечує лише конфіденційність. У комерційних організаціях щодо можливих матеріальних втрат питання цілісності, доступності та нагляду часто-густо більш критичні.

У спрощеному вигляді аналіз ризику для фірми зводиться до відповідей на такі питання: Що може загрожувати нашим інформаційним ресурсам (комп'ютерам, засобам зв'язку, даним і т. д.)? Який ступінь реальності цих загроз, або що може трапитись з тим чи іншим інформаційним ресурсом? Якщо це відбудеться, то наскільки тяжкими будуть наслідки? Які розміри шкоди та втрат? Як часто слід чекати таких проблем?

Ризики та загрози визначають набір послуг для фірми з інформаційної безпеки. Замовник з виконавцем складають так звані функціональні профілі захисту інформації (набори послуг) у вигляді спеціальних нормативних документів, яким дається ім'я та чисельний ідентифікатор. Вибір залежить перш за все від умов функціонування організації, профілю діяльності, особливостей ринкового оточення та завдань середньо- та довгострокової стратегічної перспективи бізнесу. Головне, щоб у результаті такого аналізу став можливим реальний та ефективний вибір послуг з "меню" BS7799 відповідно до компонентів єдиних критеріїв, що оформлюється у вигляді Декларації з використання.

Після етапу планування та розробки системи інформаційної безпеки починається період впровадження (проект захисту), термін якого залежить від об'єму послуг, що надає виконавець замовнику. Систему менеджменту інформаційної безпеки неможливо просто "встановити" як новий комп'ютер або програмний пакет, вона є частиною системи загального управління фірми і стосується всіх рівнів організації від вищого керівництва до виконавців.

Проект захисту – це сукупність задач захисту, функціональних вимог, вимог адекватності специфікацій засобів захисту та їх обґрунтування і є узгодженим положенням для кваліфікованого аналізу та сертифікації користувача інформаційної технології (IT-продукту).

Поняття адекватність – це показник, що реально забезпечує рівень безпеки та відображає ступінь ефективності та надійності співвідношення реалізованих засобів захисту та його попередньо поставлених завдань. Він регламентує всі етапи проектування, створення та експлуатації IT-продукту. Всього визначається 7 стандартизованих рівнів адекватності, які відповідають можливостям засобів контролю та верифікації, що використовуються у процесі розробки та вдосконалення IT-продукту.

Об'єкт оцінки (ОО) визначається як продукт або система інформаційних технологій, а також пов'язана з ними управлінська та дорадча документація, що є частиною процесу оцінки безпеки інформаційних технологій.

Концепція стандарту BS7799 спрямована на задоволення інтересів трьох основних суб'єктів проекту захисту (безпеки інформації): споживач ОО, розробник ОО та експерти по оцінці безпеки ОО.

Кінцевий узгоджений документ надасть можливість іншим особам фірми вирішувати свої задачі: офіцерам по безпеці, аудиторам, адміністраторам оцінки, особам, відповідальним за акредитацію.

Для забезпечення найбільшого ступеня відповідності між результатами процесів оцінки, що здійснюються окремими експертами, дуже важливо, щоб оцінка проводилась на спільній методологічній основі з використанням надійних та апробованих схем та методик оцінки.

Стандарт BS7799 включає три типи оцінки: оцінка профілю захисту, оцінка проекту захисту та оцінка об'єкта захисту. Щодо загальної методології, що використовується для оцінки, то вони викладені в документі CEM-97\017 – "Загальна методологія оцінки безпеки інформаційних технологій". Сферою використання положень CEM-97\017 є принципи, процедури та процеси оцінки інформаційної безпеки, а також заходи та комплекс робіт, що виконуються впродовж оцінки, розробки та контролю оцінки інформаційної безпеки. У документі визначаються такі принципи оцінки інформаційної безпеки: принцип співвідношення зусиль та заданого рівня адекватності оцінки; принцип неупередженості оцінки; принцип об'єктивності оцінки; принцип повторності та підновленості; принцип вірогідності та достовірності.

Реалізація вищезазначених принципів передбачає виконання таких умов: 1. Вартісна ефективність оцінки полягає в тому, що цінність результатів оцінки повинна компенсувати витрати тимчасових, невідворотних чи неминучих матеріальних та інших ресурсів на проведення оцінки фірмою. 2. Методика оцінки повинна мати можливість адаптуватися до мінливих умов та бути гнучкою щодо інформаційних технологій, що розвиваються. Це дозволить забезпечити відповідний рівень ефективності методів оцінки та гарантувати їх придатність до оцінки профілів захисту об'єкта оцінки. 3. Повторна доступність результатів, коли об'єкт оцінки або профіль захисту є інтегрованими частинами інших об'єктів або систем захисту. 4. Врешті, важливо забезпечити, щоб усі сторони в процесі оцінки користувалися єдиною методологією.

Кожна зі сторін, що бере участь у процесі оцінки на основі загальної методології, несе спільну відповідальність за виконання окремих задач. CEM-97\017 визначає таку відповідальність, загальні принципи та допускає, що схеми оцінки можуть вводити додаткові вимоги до сторін відповідно до особливостей національного законодавства та положень керівних документів сфери управління всередині фірми.

BS7799 є добровільним стандартом, тобто держави, де BS7799 адаптований, не вимагають його обов'язкового виконання відповідними суб'єктами всередині країни. Взагалі, у цьому нема необхідності – виконання стандарту вигідно у першу чергу самому підприємству. Однак, як і інші добровільні стандарти (наприклад, стандарт якості ISO 9000 або екологічний стандарт ISO 14000), BS7799 використовується в контрактах та комерційних угодах. У всіх випадках партнерам та клієнтам підприємства важливо знати, яким чином на підприємстві забезпечується інформаційна безпека. У цьому випадку відповідність стандарту може бути однією з умов контракту.

Формальне підтвердження відповідності стандарту дає акредитована сертифікація. Володарем британської сертифікаційної схеми є BSI (від імені Департаменту по торгівлі та промисловості Об'єднаного Королівства), який і встановлює "правила гри". У країнах, що прийняли аналоги BS7799, відповідно існують свої схеми сертифікації, у рамках яких і працюють місцеві аудитори. Там, де аналоги BS7799 відсутні (у т. ч. і в Україні), у принципі можна використовувати будь-які зовнішні схеми. Але оскільки британська схема є найбільш старою та розвиненою, то за інших рівних умов, перевагу віддають саме їй.

Для одержання сертифікату системи менеджменту інформаційної безпеки підприємство (організація, фірма) оцінюється аудитором BS7799. Аудитор не може одночасно бути і консультантом. З приводу цього існують досить жорсткі правила. Аудит по BS7799 складає аналіз документації по системі менеджменту інформаційної безпеки, а також вибіркового контролю в організації, який дозволяє впевнитися, що реальна практика відповідає опису системи.

Акредитовану сертифікацію можуть надати лише ті сертифікаційні товариства, що пройшли акредитацію BSI. З вересня 2003 р. вперше в Україні таке право має представництво Bureau Veritas, а сертифікат стандарту

BS7799 та ISO17799, що нею видаються, беззастережно визнається на міжнародному рівні. Впровадження в Україні міжнародних апробованих схем оцінки безпеки в рамках загальних критеріїв та принципів дозволить не лише оцінити власні продукти та системи, а й активно брати участь в оцінці виробів, продуктів та систем іноземного виробництва, що дасть змогу реально захистити національний ринок від недоброякісної продукції.

Згідно з прогнозом, наступні десять років в Україні будуть періодом стрімкого зростання попиту на сертифікацію відповідно до стандартів BS7799 та ISO17799, оскільки темпи росту електронної комерції будуть значно випереджати темпи росту інших секторів та сегментів ринку. Одночасно значний інтерес до сертифікації будуть виявляти й інші сектори комерційної та державної діяльності: банки, фінансові та страхові компанії, торговельні фірми, телекомунікаційні компанії, туристичні фірми, державні податкові органи та органи внутрішніх справ, медичні заклади, підприємства транспорту тощо. Швидкий розвиток BS7799 та значний інтерес до нього свідчить про те, що відповідність новому стандарту інформаційної безпеки стане важливою умовою комерційного успіху в найближчій перспективі.

1. ISO\IEC 15408-1:2000 – Information technology – Security techniques – Evaluation criteria for IT sector – Introduction and general model. 2. ISO\IEC 15408-1:2001 – Information technology – Security techniques – Evaluation criteria for IT sector – Security functional requirements. 3. ISO\IEC 15408-1:2002 – Information technology – Security techniques – Evaluation criteria for IT sector – Security assurance requirements. 4. CEM-97\017. Common Evaluation Methodology for Information Technology Security – Part 1: International general model. 5. ISO\IEC 7498-2: 1999. – Information processing systems – Open Systems Interconnection – Basic Report – Part 2: Security Architecture.

Надійшла до редколегії 29.03.04

Я.В.Томашик, асп.

ГЛОБАЛЬНІ ТЕНДЕНЦІЇ РОЗВИТКУ РИНКІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ: КАЛІФОРНІЙСЬКИЙ ШЛЯХ

На основі останніх даних проаналізовано зміни в індустрії електроенергетики, набутий у ході реформ досвід окремих ринків, насамперед досвід Каліфорнії, а також підсумовано ключові фактори, що впливають на напрямок глобальних реформ та основні моделі реформованих ринків.

The changes in the industry, the experience acquired, and primarily in California, are studied. Some key factors that influence the direction of global reforms and basic models of the reformed markets.

Протягом останніх п'ятнадцяти років загострилися дискусії щодо доцільності та шляхів реформування секторів економіки, яким більшою чи меншою мірою притаманні риси природних монополій. Метою даної роботи є аналіз факторів, що зумовлюють напрямок розвитку електроенергетики, їх вплив на тенденції сектору з погляду структури та характеру відносин усіх його учасників.

Необхідність проведення реформ була продиктована намаганнями підвищити ефективність кожної складової всього господарського комплексу, яка полягала в низькій ефективності та конкурентоспроможності промисловості в масштабі цілих країн. Ця необхідність була викликана низкою економічних, технологічних та соціальних факторів, а також міркуваннями захисту навколишнього середовища.

Важливість економічних факторів зумовлена тією роллю, яку почала відігравати електроенергетика в економіці країн світу. Електроенергія стала важливою складовою частиною виробництва багатьох товарів та послуг, особливо у сфері інформаційних технологій. Також до економічних факторів можна віднести обмеженість державного фінансування в здійсненні потрібного обсягу інвестицій в електроенергетику з метою покриття зростаючого попиту.

Технологічними факторами, що спонукають до реформування, є зниження мінімального ефективного розміру генератора енергії, покращення якості передавальних мереж та розвиток інформаційних технологій, що поліпшив можливості управління та синхронного оперування, а також обліку в електроенергетичних системах окремих країн.

Головними соціальними факторами, що вплинули на необхідність реформ, стала потреба забезпечити безперебійність енергопостачання, надійність енергосистем взагалі при одночасному розширенні можливостей споживачів при виборі постачальника електроенергії.

І, нарешті, до останньої групи факторів належать природоохоронні фактори, серед яких чільне місце посідає необхідність стимулювання розвитку енергозберігаючих технологій з боку споживання та екологічно безпечних технологій виробництва електроенергії з боку її генерації.

З теоретичного погляду передача та розподіл електроенергії становлять те ядро електроенергетичної системи, якому притаманні всі властивості природної монополії [1]. З іншого боку, такі види діяльності, як генерація та постачання електроенергії кінцевим споживачам, за певних умов мають всі передумови для розвитку в них конкурентних ринкових відносин. Залежно від ступеня лібералізації окремих видів діяльності в світовій практиці в останнє десятиріччя сформувалися три базові моделі ринку електричної енергії [2]. Механізм функціонування моделі вільного доступу передбачає гарантування власником мережі електропередач недискримінаційного вільного доступу до мережі для конкурентів. За цією моделлю існуючі вертикально інтегровані утворення (генерація-передача-розподіл) не обов'язково мають бути розформовані в окремі структури.

Наступна модель (модель конкурентного пулу або модель білатеральних контрактів із обов'язковим спотовим ринком) поєднує в собі принципи недискримінаційного доступу до мережі та конкурентного спотового оптового ринку енергії. Крім того, повинна існувати достатня кількість незалежних генераторів, оскільки спотова ціна за такої форми організації ринку встановлюється на регулярних аукціонах серед учасників пулу.

Існують також і варіанти останньої моделі – моделі єдиного покупця, суть якої полягає в існуванні обов'язкового оптового ринку електроенергії та єдиного покупця, що закуповує всю електроенергію у виробників за диференційованими цінами та реалізує її розподільчим компаніям за єдиною ціною в кожен момент часу.

Найбільш показовим та повчальним щодо можливих негативних наслідків невдалої реформи в секторі енергетики є приклад штату Каліфорнія. На початку реформ серед основних завдань ставилися забезпечення надійного електропостачання за низькими та стабільними цінами, проте результатом реформ стало різке зростання цін на електроенергію, нездатність генеруючих компаній забезпечити належний об'єм електропостачання, що призвело до плаваючих відключень електроенергії влітку 2000 р. Задля відповіді на питання, в чому причина згаданих вище явищ, необхідно проаналізувати ключові фактори реформ, якими стали невдалий дизайн структури ринку, зростаючий попит на електроенергію темпами, що значно перевищували здатність