УДК 004.056 **Єжова Л.Ф. (ДУІКТ)**

«14Р» ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІЗ ВИКОРИСТАННЯМ МАРКЕТИНГОВОГО ІНСТРУМЕНТАРІЮ

У статті побудовано модель інформаційної безпеки за допомогою маркетингового підходу. Запропонована множина факторів, що впливають на рівень інформаційної безпеки, на основі яких цю модель можна досліджувати методами факторного та кореляційного аналізу, встановлювати рейтинги факторів для кожної конкретної інформаційної системи.

Вступ

Управління інформаційною безпекою – важливий вид діяльності, метою якого є контроль процесів забезпечення інформацією і запобігання її несанкціонованому використанню.

Побудова моделі управління інформаційною безпекою, адекватної до реальних інформаційних процесів організації, дозволить забезпечити рівень їх захисту, визначений політикою інформаційної безпеки організації.

Існують 4 підходи до управління підприємством (організацією):

- процесний підхід в управлінні;
- системний підхід в управлінні;
- ситуаційний підхід в управлінні;
- підхід з позицій різних шкіл в управлінні.

Останнім часом в ринковій економіці успішно використовується маркетинговий підхід до управління підприємством.

Метою цієї роботи є спроба застосувати маркетинговий підхід для теоретичного дослідження проблем управління інформаційною безпекою та практичного застосування отриманих результатів.

Історія питання

Термін «маркетинг-мікс» винайшов Ніл Борден у 1953 році, після цього з посібника Джерома Маккарті в 1960 році маркетологи вперше познайомились з 4Р (Product – продукт, Price – ціна, Place – розміщення, Promotion – просування). Найбільше розповсюдження модель 4Р отримала завдяки Ф.Котлеру та його посібникам і монографіям. Ця ідея виявилася настільки плідною, що на багато років затвердила саме цей підхід до вивчення маркетингу та його практичного застосування.

Але згодом, з розвитком інформаційних технологій, із зростанням ролі персоналу у реалізації будь-яких процесів, стало зрозуміло, що в рамках 4Р нема повного охвату проблем, пов’язаних із маркетинговою діяльністю підприємства. Тоді з’явилися пропозиції від різних авторів доповнити комплекс 4Р новими складовими (people, personal, process тощо).

Але були й супротивники цих новацій, вони доводили, що ці нововведені «Р» можна вважати тільки перефразуванням тих самих «Р» Ф.Котлера.

Модель, розроблена Д. Ратмелом в 1974 г. [1], була першою спробою показати різницю між функціональними задачами маркетингу у виробничому секторі (продуктів) та невиробничому (послуг), а отже існують три, хоч і пов’язаних, але цілком самостійних процеси:

1) процесс виробництва послуг;

2) процесс маркетингу цих послуг;

3) процес споживання цих послуг.

Функціональні задачі маркетингу в цій системі:

- необхідно організувати процес виробництва тих послуг, які задовольнять потреби користувача;

– необхідно розробити стратегії комунікації, каналів розподілу, щоб ефективно просувати ці послуги користувачу;

– необходідний моніторинг процесу споживання послуг з метою вивчення поведінки користувачів, виявлення нових потреб та повного їх задоволення.

Французька модель П. Эйгліє та Е. Лангеарда (взагалі, більш правильно казати Е. Ланжарда), розроблена у 1976 р., підкреслила не тільки одночасність виробництва і споживання послуги, але й розділила персонал на контактний (персонал фірми) та неконтактний (споживачі, що контактують із персоналом) [2].

Ключовими факторами в цій моделі є:

1) сам процес обслуговування;

2) організація послуг;

3) споживач А – цільовий ринок послуг;

4) споживач Б - що контактує зі споживачем А.

У французькій моделі маркетингу послуг, в якій крім традиційних стратегій маркетингу, що використовуються у виробничому секторі (товар, ціна, комунікації, канали розподілу), виділяють три додаткові стратегії.

Перша – створення певного матеріального середовища, за яким контактний персонал буде намагатися оцінити якість майбутнього обслуговування, що є складовою частиною способу доведення послуги до споживача - персоналу, що не є контактним.

Друга – забезпечення певних стандартів поведінки персоналу, що знаходиться в контакті з споживачем в процесі обслуговування.

І, нарешті, третя – забезпечення такої організації споживачів, при якій кожний з них знаходився б «серед своїх» груп споживачів.

У 1981 році Бумс і Бітнер запропонували модель 7Р, доповнивши модель 4Р трьома додатковими Р: process, physical evidence, people (процес, матеріальний доказ і люди) [3]. Потім у 1984 році Філіп Котлер запропонував public relations и political power (політична воля), а потім у 2000 році додав ще одну компоненту – packaging (упаковка).

Е.Боуман запропонував використати цей підхід (як інструмент) до вивчення зовсім іншої проблеми, а саме до державної стратегії в освітній системі (5Р), але при цьому він вклав у ці 5Р зовсім новий зміст [8]. Стратегія, на його думку – це такі «5Р»:

Plan (план) – свідомо вибрана послідовність дій;

Ploy (маневр) – обхід конкурента;

Position (позиція) – місцезнаходження в середовищі;

Perspective (світогляд) – особистий спосіб світосприйняття;

Preference (перевага) – забезпечення конкурентної переваги.

Як бачимо, ідея розширення Р-факторів виявилася дійсно плідною.

Отже цілком можливе і доцільне використання маркетингового інструментарію для оцінки характеристик окремих складових будь-якого процесу діяльності, для дослідження категорій, які не є маркетинговими.

Побудова моделі інформаційної безпеки

Щоб визначити, скільки «Р» впливають на рівень інформаційної безпеки, введемо позначення для понять, що є основними факторами інформаційної безпеки:

Product – продукт, послуга інформаційної безпеки (P_1);

Price – ціна засобів і заходів захисту інформації (P_2);

Place – місце інформаційної безпеки в організації (P_3);

Promotion – просування засобів і заходів захисту інформації в організації (P_4);

Personnel – персонал контактний з інформаційними процесами (P_5);

People – особи, що не є персоналом контактним з інформаційними процесами (P_6);

Physical premises – інфраструктура інформаційної безпеки (P_7);

Politics – політика інформаційної безпеки (P_8);

Program – програма інформаційної безпеки (P_9);

Process –процес управління інформаційною безпекою (P_{10});

Power – повноваження, рівень доступу (P_{11});

Position – позиція керівництва до проблем інформаційної безпеки (P_{12});

Public relation – зв'язок із персоналом (P_{13});

Preference – забезпечення конкурентної переваги (P_{14}).

Якщо розглядати стратегію управління інформаційною безпекою (Process), то вона пов'язана з інформаційними процесами, персоналом контактним з інформаційними процесами (Personnel) та зовнішнім до інформаційних процесів середовищем, що складається із споживачів інформації, конкурентів, партнерів, осіб, «зацікавлених» у конфіденційній інформації, тощо (People). До зовнішнього середовища інформаційних процесів можна віднести і персонал компанії, що не є контактним персоналом, прирівнюючи їх до споживачів інформації.

Відповідно до цього необхідно контролювати три ланки:

Process – Personnel;

Process – People;

Personnel – People.

Отже треба забезпечити необхідний рівень інформаційної безпеки для кожної з цих ланок і, в першу чергу, визначити для контактного персоналу (Personnel) відповідні повноваження та рівні доступу (Power). У процесі функціонування організації будь-які зміни в інформаційній системі викликають необхідність змін у політиці інформаційної безпеки (Politics), програмі інформаційної безпеки (Program), перерозподіл повноважень та зміни рівнів доступу.

У наш час багато які організації мають справу з інформаційною безпекою на стратегічному рівні – з політикою інформаційної безпеки (Politics) та інформаційним плануванням (Program) і на операційному рівні - при виборі засобів забезпечення безпеки. Вони недостатньо уваги приділяють саме процесу управління інформаційною безпекою, безперервному аналізу та реалізації результатів аналізу у формі технічних рішень, підтримці ефективності заходів безпеки при зміні вимог і середовища. Отже, організація процесу управління інформаційною безпекою головним чином залежить від ставлення керівництва до проблем інформаційної безпеки, тобто від позиції, яку займає керівництво організації (Position).

Наслідком розриву між операційним і стратегічним рівнями є те, що на тактичному рівні значні кошти можуть вкладатися у заходи безпеки, які вже не є актуальними, замість вкладання коштів у більш ефективні заходи.

Процес управління інформаційною безпекою входить до сфери компетенції загальної інформаційної безпеки, задачею якої є забезпечення збережності інформації - захищеності від відомих ризиків і, наскільки це можливо, уникнення невідомих ризиків.

Задачею процеса управління інформаційною безпекою (Process) є постійне забезпечення безпеки інформаційних послуг на рівні, визначеному політикою безпеки (Politics), забезпечення прийняття ефективних заходів з інформаційної безпеки на стратегічному, тактичному та операційному рівнях.

Процес управління інформаційною безпекою необхідний для підтримки неперервного функціонування організації. Безпека у наш час є важливійшим показником якості менеджменту.

Функціональні задачі маркетингу в системі Д. Ратмела цілком корелюють із задачами організації інформаційної безпеки, а саме:

– необхідно організувати процес виробництва послуг із захисту інформації, які задовольнять потреби забезпечення заданого рівня інформаційної безпеки;

– необхідно розробити стратегії комунікації, каналів ефективного просування послуг із захисту інформації до контактного персоналу;

– необхідний моніторинг процесу споживання послуг із захисту інформації з метою вивчення поведінки контактного персоналу, виявлення нових потреб у захисті інформації та повного їх задоволення.

Що стосується стратегії комунікацій, то зважимо, що складність IT-інфраструктури (Physical premises) постійно зростає, а це означає, що функціонування будь-якої організації стає більш уразливим до технічних збоїв, помилок персоналу (Personnel), зловмисних дій хакерів і зломщиків (People), комп'ютерних вірусів тощо. Ця зростаюча складність вимагає уніфікованого підходу до управління інфраструктурою – однією з важливіших складових інформаційної безпеки.

Забезпечення інформаційної безпеки відноситься до допоміжної діяльності підприємства і є витратною статтею. А щоб ці витрати були недаремними, необхідно спільно дотримуватись всіх вимог інформаційної безпеки організації. Інтереси керівництва організації у сфері інформаційної безпеки та всіх її співробітників в ідеальному варіанті повинні співпадати.

Але, взагалі кажучі, інтереси співробітників – кінцевих користувачів (Personnel) полягають у наявності цілісної та доступної інформації, а також нормального функціонування інформаційної інфраструктури для безперебійного виконання їх професійних обов'язків. Крім того, вони просто повинні дотримуватись всіх вимог інформаційної безпеки, за що і несуть відповідальність. Інші проблеми інформаційної безпеки їх не обходять. Тому керівництво організації повинно подбати про мотивацію і стимуляцію цієї категорії персоналу для виконання всіх вимог інформаційної безпеки, для навчання і перенавчання при впровадженні нових технологій, засобів і заходів інформаційної безпеки, для запобігання плинності кадрів, витоку та пошкодження інформації.

У французькій моделі маркетингу існують групи споживачів з однаковими вимогами до послуг. У сфері інформаційної безпеки це може бути трансформовано у групи представників контактного персоналу з однаковими рівнями доступу – введення рольового доступу.

Управління інформаційною безпекою невід'ємне від проведення аналізу ризиків загроз інформаційній безпеці організації. В процесі аналізу ризиків беруть участь керівники організації та деякі структурні підрозділи організації: підрозділи основних бізнес-напрямків (через конкурентну боротьбу), підрозділи управління інформаційною інфраструктурою, підрозділ управління інформаційною безпекою. Їх взаємодія дозволить успішно проводити аналіз і оцінку ризиків та ефективно використовувати їх результати у подальшому. Ця категорія контактного персоналу теж повинна бути по-іншому вмотивована щодо підтримки необхідного рівня інформаційної безпеки.

Політика управління ризиками організації – найважливіше питання, оскільки вона задає пріоритети об'єктів захисту, одним з яких є стратегічне управління конкурентоспроможністю організації (Preference).

Public relation – це одна із найважливіших складових інформаційної безпеки, оскільки без постійного і наполегливого нагадування про необхідність дотримання всіх вимог інформаційної безпеки, без роз'яснення переваг від використання засобів і заходів інформаційної безпеки, рівень інформаційної безпеки неминуче почне деградувати.

Отже, виходячи з усього вище згаданого, можна запропонувати модель інформаційної безпеки МІБ як функціонал F від усіх перелічених факторів інформаційної безпеки P_i , i = 1, ..., 14 :

$$МІБ = F (P_1, P_2 , \dots , P_{14}).$$

Звичайно, ця множина факторів у разі необхідності може бути доповнена ще іншими факторами або можливе нехтування деякими наведеними факторами. Таку модель можна досліджувати методами факторного та кореляційного аналізу, встановлювати рейтинги факторів для кожної конкретної інформаційної системи.

Висновки

У статті аналізується розвиток моделювання маркетингу з використанням різних його складових.

Використовуючи маркетинговий інструментарій для оцінки характеристик окремих складових інших процесів діяльності, запропонована множина факторів, від яких залежить рівень інформаційної безпеки, та на їх основі побудовано модель інформаційної безпеки, яку можна досліджувати методами факторного та кореляційного аналізу, встановлювати рейтинги факторів для кожної конкретної інформаційної системи.

Література

1. Rathmell, J. Marketing in the Service Sector. — Mass: Winthrop Publishers, 1974.

2. Eiglier, P. and Langeard, E Principles de politique marketing pour les enterprises de services. — L'Institute d'Administration des enterprises, Universite d'Aix-Marselle, 1976.

3. Bitner M., Zeithaml V. Services marketing. — Massachusetts, 1996.

4. Lovelock C. Services marketing. — London, 2001.

5. Bitner, M. J. Servicecapes: The impact of Physical surrounding on Customer and Employees. Journal of Marketing. — 1992. — 56 (April).

6. Ворачек Х. О состоянии «теории маркетинга услуг» // Проблемы теории и практики управления. — 2002. — № 1.

7. Котлер Ф. Маркетинг, гостеприимство, туризм. — М., 1998.

8. Новаторов Э. Международные модели маркетинга услуг // Маркетинг в России и за рубежом. — 2000. — № 3.

Надійшла: 08.06.2011 р.

Рецензент: д.т.н., проф. Квасніков В.П.