

ТЕЗИ ВИСТУПІВ

Вишня В.Б. - професор кафедри
Дніпропетровського державного
університету внутрішніх справ,
доктор технічних наук, професор;
Гавриш О.С. - викладач
Дніпропетровського державного
університету внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

При розгляді питання про інформаційно-аналітичне забезпечення безпеки підприємства ми можемо зустрітися з двома підходами до її організації. Відповідно до першого вважається, що інформаційно-аналітичним забезпеченням безпеки діяльності фірми повинна займатися безпосередньо сама фірма. Інформаційний підрозділ при цьому є структурним підрозділом організації, має прямий вихід на директора (власника) і сам будує стосунки з іншими структурними підрозділами, у тому числі і його службою безпеки.

Міжнародний досвід показує, що такий підхід характерний для великих корпорацій, тих, хто займається виробництвом і реалізацією продукції. Така організація інформаційно-аналітичного забезпечення виробничої діяльності пов'язана з тим, що основні ризики і погрози породжуються комерційною діяльністю конкурентів, виходять із змін стану ринків і тому подібних обставин.

В даному випадку таку інформаційно-аналітичну роботу ведуть конкретні фахівці. Взаємодія інформаційно-аналітичного підрозділу із службою безпеки у такому разі полягає в тому, що служба повідомляє аналітиків про можливість загрози з боку кримінальних структур та ін. Аналітики ж орієнтують службу безпеки про характер змін в ризиках бізнесу, виникненні нових викликів, певних погроз і їх суб'єктах, орієнтують підрозділи, які зайняті пошуками інформації відносно напрямів її пошуків, розвідувальних і контррозвідувальних заходів [1]. Подібна організація інформаційно-аналітичної роботи використовується в великих брендових корпораціях.

Відповідно до іншого підходу – інформаційно-аналітичний підрозділ (група або окремих аналітик) мають бути включені до складу служби безпеки організації. В цьому випадку аналітики структурно входять в службу безпеки і підкоряються безпосередньо начальникові служби безпеки, який, як правило, виконує і роль головного аналітика. Безпосередній вихід на керівництво фірми має тільки керівник служби безпеки.

Така організація інформаційно-аналітичного забезпечення безпеки підприємства характерна для більшості вітчизняних кредитно-фінансових

установ, торговельних і посередницьких підприємств регіональних і міжрегіональних рівнів. Зусилля при цьому концентруються на необхідності протистояти неправомірним погрозам з боку дій конкурентів, і значним погрозам з боку кримінальних структур, а останнім часом необхідності протистояти можливим рейдерським атакам.

Аналітична робота в цьому випадку покладається на досвідчених фахівців у сфері недержавної безпеки, які повинні мати професійні знання у сфері діяльності підприємства. До сьогодні таких фахівців готували з працівників структур, які виявили інтерес і здібності до аналітичної роботи. Зараз все частіше на такі посади приходять фахівці, які здобули вищу освіту у ВНЗ, що готують фахівців з безпеки. Окрім фахівців сфери діяльності підприємств для проведення конкурентних аналітичних розробок і експертиз іноді притягуються вузькі фахівці: психологи, інженери і технологи, соціологи, прикладні математики і програмісти, криміналісти і т.ін. Подібна організація інформаційно-аналітичного забезпечення безпеки недержавних структур зараз використовується практично в усіх банках, страхових компаніях.

При будь-якій діяльності необхідно враховувати, що інформаційно-аналітичне забезпечення безпеки підприємства повинне вестися однією структурою. Паралельно аналітична робота служби безпеки і власне підприємства практично не допустима. Це зв'язано з тим, що інформаційне поле дійсно буває істотно обмеженим, тому робота декількох структурних підрозділів в одному і тому ж напрямі може бути легко виявлена, прорахована (конкурентами, або злочинними угрупованнями) і припинена або паралізована.

В той же час, не виключається варіант такої організації інформаційно-аналітичного забезпечення безпеки виробничій діяльності, коли аналітична група діє на правах самостійного структурного підрозділу підприємства, підкоряється паралельно директорові і начальникові служби безпеки. Як правило, при цьому назва групи зашифровується: група вивчення ринку, відділ маркетингу, інформаційно-довідкова служба і так далі.

Декілька слів про функції інформаційно-аналітичного підрозділу, що забезпечує безпеку підприємства. Вони можуть бути досить великими, але на практиці вони зведені до тих цілей і завдань, які зараз стоять перед організацією.

У будь-якому випадку сьогодні аналітики повинні:

- вивчати кон'юнктуру ринку;
- вести збір, накопичення, обробку і переробку інформації (про можливих клієнтів, партнерів, перспективи співпраці, конкурентів, рейдерські структури і їх діяльність), її видачу на запит правоохоронних підрозділів і керівництва фірми;
- збирати і обробляти інформацію про процеси, що відбуваються в кримінальних структурах, про кримінальну обстановку в районі (регіоні), її впливі на діяльність підприємства;
- розробляти рекомендації і ефективні заходи протистояння

злочинним посяганням, спрямованим проти інтересів фірми, її співробітників, її активів, землі і, загалом, власності;

- сприяти кадровому відділу у вивченні кандидатів, підборі співробітників, постійному моніторингу їх діяльності за межами організації;
- контролювати діяльність партнерів і клієнтів, з'ясовувати питання їх надійності, платоспроможності, майнового і фінансового положення, визначати їх дійсні наміри;
- брати участь в діяльності служби безпеки фірми в справах повернення боргів, кредитів і вирішеннях інших проблемних питань, що виникають в повсякденній діяльності організації;
- надійно забезпечувати діяльність захисту інформації з обмеженим доступом.

Якщо у Вашій організації буде можливість мати декілька співробітників, які займатимуться інформаційно-аналітичній забезпеченням безпеці підприємства, то виникне можливість деякої спеціалізації аналітиків. Частина з них орієнтується на збір інформації, це так звані збирачі. А частина – займається узагальненням, класифікацією, аналізом, збереженням і видачею інформації, аналітичних матеріалів – інформаційних документів. Саме ці співробітники орієнтують збирачів про те яку інформацію треба збирати, де її можна знайти і тому подібне. Значна частина роботи по збору інформації кладеться на плечі збирачів. Саме вони використовуючи свої можливості, можливості інших категорій співробітників фірми, можливості, які відкриваються всесвітньою мережею Інтернет. Вони збирають інформацію про платоспроможність клієнтів, стан справ у партнерів, дані про можливі зв'язки контрагентів з мафіозними структурами, намірах конкурентів і про багато що інше.

Іноді для отримання додаткової важливої інформації доводиться користуватися послугами різних інформаційних систем і інформаційно-аналітичних агентств. За такі послуги, як правило, доводиться платити і платити немало. У крузі фахівців з безпеки вже склався своєрідний «крилатий вислів» – «За інформацію треба платити, за її відсутність доводиться розплачуватися» [2].

Рішення задачі інформаційного забезпечення безпеки власними зусиллями організації має відмінність від забезпечення її зовнішніми структурами. Власними силами відбувається рішення завдань інформаційного забезпечення конкретних проектів, що визначає наявність і конкретні підстави для збору і аналізу загальної інформації. Інформація, що добувається, повинна мати цільову спрямованість та:

- визначати ознаки виникнення і розвитку кризових ситуацій;
- давати характеристику сильним і слабким сторонам конкурентів;
- розкривати дійсні наміри потенційних і діючих партнерів відносно нашої організації;
- бути ефективною в цілях здійснення впливу на позицію зацікавлених осіб в ході переговорного процесу;

- своєчасно виявляти моменти виникнення нових викликів, і їх переростання в погрози підприємству;
- забезпечити контроль виконання партнерами досягнутих домовленостей;
- забезпечити також виявлення каналів витоку і втрати інформації з організації через вивчення змін в діяльності партнерів і конкурентів;
- стати основою для ухвалення рішення;
- орієнтувати керівництво підприємства про виникнення небезпек і сприяти організації ефективної діяльності по ліквідації наслідку негативного впливу.

І це далеко не усі питання, що повинні підніматися і відпрацьовуватися працівниками аналітичного підрозділу підприємства [3]. Треба обов'язково враховувати, що в країнах з ринковою економікою, а Україна поступово просувається в їх число, відомості про клієнтів, партнерів інші відомості прийнято вважати капіталом фірми. Списки клієнтів фірми, її партнерів і конкурентів, банки відомостей про них складаються в першу чергу зусиллями власників фірми і у будь-якому випадку – за їх рахунок. Значна частина цієї інформації надається менеджерами відділу продажів, відділу закупівель і відділу маркетингу. Аналітики повинні добре зорієнтувати персонал цих відділів, давати чіткі інструкції за яким принципом вони повинні поставляти інформацію аналітичному підрозділу.

Аналітичній групі підприємства разом з цими службами треба регулярно поповнювати спеціальний банк даних. При цьому окремим завданням аналітиків має бути строгий облік відомостей: де, як і коли отримані ці відомості, як вони були використані. Систематичне накопичення даних в належному виді з можливостями оперативного зіставлення відомостей даних з різних джерел забезпечує перевірку достовірності останніх, а також своєчасне збудження підозри про наявність дезінформації.

У нормально працюючому інформаційно-аналітичному підрозділі на кожного партнера, клієнта, конкурента накопичуються відомості про нього: – потреби і бажання, звички, стан, договори про надання йому раніше привілеїв, а також примітки, за що вони надавалися і багато інших даних.

Відносно вимог клієнта: фіксуються дані про кількість товарів і послуг, то якими способами і з використанням яких режимів відбулася доставка товарів; яка періодичність постачань, чим вони повинні доповнятися, інформації про оплати, а також інші специфічні особливості контрактів з цим клієнтом. Також накопичуються дані, які визначають прибутковість усієї операції з конкретним клієнтом (об'єми трансакції, що очікуються, частота постачань, зміна цін, розпродажі, які плануються).

У завдання аналітичного підрозділу входить орієнтація продавців послуг і товарів, які випускаються фірмою, на надання письмових звітів конкретним клієнтам по кожному факту продажів. У таких звітах можуть бути відображені перспективи майбутніх продажів.

Відповідна інформація має бути впорядкована, сконцентрована у керівництва організації, а також мати конфіденційний характер (навіть

характер комерційної таємниці).

Завдання аналітиків певним чином орієнтувати працівників відділу маркетингу своєї фірми. Вивчаючи клієнтів, вони зобов'язані збирати і аналізувати дані про конкурентів. Саме аналітики повинні пропонувати їм план такої діяльності: – які відомості необхідно збирати, де і як ці дані добуваються і відображуються, які дії персоналу організації для цього потрібні, як вирішуються проблеми при отриманні необхідних відомостей. Разом з цим необхідно враховувати: час, місце, спосіб отримання, їх стосунки до об'єктів, які вивчаються, до дій, що прогножуються і які обумовлюються змістом інформації.

Якщо ми обізнані про найбільш прибуткових клієнтів конкурента, то у нас з'явиться шанс перемогти останнього, переманивши його клієнтуру. Значення має особиста інформація про клієнтів: а саме, дані про їх прив'язаності, дружні і інші зв'язки в середовищі підприємців і конкурентів, особливо такі, які впливають на процес ухвалення рішень про підтримку ділових стосунків з організацією або про їх припинення.

У літературі є різні варіанти списків основних напрямів збору інформації, які охоплюють практично усі аспекти діяльності підприємства-партнера і підприємства-конкурента [4].

Приведемо узагальнений список:

1. Інформація про ринок:

- ціна, умови угод, специфіка продукту, знижки;
- об'єм, тенденція і прогноз збуту конкурентного продукту;
- частина ринку і тенденції його зміни;
- ринкова політика і плани;
- стосунки із споживачами і репутація;
- чисельність і розставлення торговельних агентів;
- канали, політика і методи збуту;
- постановка реклами.

2. Інформація про виробництво продукції:

- оцінка якості і ефективності;
- номенклатура виробу;
- технологія і устаткування;
- рівень витрат;
- виробничі потужності;
- спосіб упаковки;
- доставка;
- розміщення і розмір виробничих підрозділів і складів;
- можливості проведення науково-дослідних робіт.

3. Інформація про організаційні особливості і фінанси:

- виявлення осіб, які приймають ключові рішення;
- філософія осіб, які приймають ключові рішення;
- програми розширення і придбань;
- головні проблеми і можливості їх рішення;

- програми проведення науково-дослідних робіт.

Звичайно, заведений перелік не є повним, він тільки орієнтує відносно напрямів отримання, накопичення, обробки і перетворення інформації необхідної для надійного інформаційно-аналітичного забезпечення безпеки підприємства.

Використані джерела:

1. Герасимчук А., Тимошенко О., Шашкевич Я. Етика і етикет сучасного бізнесу – запорука економічної безпеки підприємств: навч. посіб / за заг. Ред.. З.І. Тимошенко - К.: Вид-во Європ. ун-ту, 2007. - 285 с.
2. Позднишев Є.В. Інформаційно-аналітичне забезпечення безпеки підприємництва «Методи та їх застосування»: Навч. посібник. Книга 1.-К.: Видавець Позднишев, 2007 р. - 76 с.
3. Романчев Н.Р., Нежданов И.Ю. Конкурентная разведка. Практический курс – М.: «Ось - 89», 2007. – 272 с.
4. Чергенець Е.В., Зайцев А.В., Позднишев Є.В. Інформаційно-аналітичне забезпечення безпеки підприємництва «Збір та пошук інформації»: Навч. посібник. Книга 2. – К.: Видавець Позднишев 2007. – 74 с.

Воронов І.О. – доктор юридичних наук, старший науковий співробітник, адвокат АО "Саенко Харенко (м. Київ)

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

Розвиток високих інформаційних технологій являє собою масштабний динамічний процес, який має постійний та цілеспрямований характер. Внаслідок цього невпинно удосконалюються і створюються нові засоби та способи обробки інформації, підвищується швидкість передачі даних, з'являються нові види каналів зв'язку, виникають раніше невідомі або недосяжні послуги.

Інформатизація суспільства надала кожному її члену можливість користуватися такими здобутками для повноцінної життєдіяльності та функціонування у сучасних умовах. Неможливість здійснення вибіркової у розповсюдженні й впровадженні здобутків високих інформаційних технологій призвела до того, що кримінальні структури стали їх активним необмеженим споживачем. Таким чином вони отримали гнучку структуру управління, високу пластичність індивідуальної й організованої кримінальної діяльності, специфічну інфраструктуру. Це також призвело до виникнення нових видів кримінальних діянь і певного поширення числа потенційних потерпілих. Аналіз законодавства, опублікованих точок зору, матеріалів практичної діяльності вітчизняних правоохоронних підрозділів, а також правоохоронних органів зарубіжних країн свідчить про те, що в сучасних умовах ефективно забезпечення кібербезпеки України неможливе без врахування специфіки та системного підходу.

Незважаючи на численні публікації, на даний час й досі бракує