УДК 004.056.53:621.39

В.І. ЗАБОЛОТНИЙ, канд. техн. наук, А.В. ЄРМОЛОВИЧ

МЕТОДИКА ОРГАНІЗАЦІЇ ЗАХОДІВ ЗАХИСТУ ВІД ТЕХНІЧНИХ ЗАСОБІВ КОНКУРЕНТНОЇ РОЗВІДКИ

Вступ

Розвиток України в економічному плані інтенсифікує процес збільшення матеріального виробництва конкурентоспроможної наукоємної продукції. Отримати суттєвий прибуток від своєї продукції власник може тільки у тому випадку, коли забезпечить раптовість її появи на відповідному ринку [1]. Суттєвим чинником для досягнення цієї мети може стати конкурентна розвідка. «Конкурентна розвідка – це реалізація системної програми збору, аналізу і розподілу інформації про діяльність конкурентів і загальні тенденції бізнесу, пов'язаних з цілями конкретної компанії» – зазначає Ю.П. Воронов [2]. У той самий час М. Логвинов зазначає, що конкурентна розвідка – це збір і обробка даних з різних джерел для вироблення управлінських рішень з метою підвищення конкурентоспроможності комерційної організації, що проводяться в рамках закону і з дотриманням етичних норм та законодавчих норм [3]. Основною проблемою в захисті від конкурентної розвідки є визначення можливих джерел витоку інформації, що становлять комерційну таємницю, несанкціоноване ознайомлення конкурентів з якої може завдати збитків. У статті 505 ЦК України визначено, що комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію, комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Постановка задачі

Основною метою проведених досліджень є визначення змістовності основних понять при захисті від конкурентної розвідки, розмежування та постанова завдань для всіх основних етапів з розробки заходів захисту від конкурентної розвідки, розробка методики організації даних робіт.

Методи конкурентної розвідки можуть бути як законними, або такими, при використанні яких відбувається порушення закону. Існує безліч можливостей, що дозволяють отримати інформацію, що становить комерційну таємницю, не прикладаючи багатьох засиль. Метод конкурентної розвідки, при якому робота ґрунтується на вивченні інформації, отриманої з офіційних опублікованих джерел: відбувається аналіз публікацій, статей, отриманих через Інтернет і ЗМІ про конкурентів, аналіз маркетингових досліджень в даній галузі (купівля минулих маркетингових досліджень конкурентів), опитування конкурентів під виглядом маркетингового дослідження, аналіз отриманих фінансових документів конкурентів, аналіз структури компанії конкурентів, аналіз статутних документів конкурентів, аналіз структур і господарських взаємозв'язків. Існує такий метод конкурентної розвідки, як «мертві вакансії»: коли запрошують на співбесіду співробітника з фірми конкурента для роботи на більш вигідних умовах. На цій співбесіді у працівника з'ясовують подробиці його діяльності. Ніяких, природно, після цієї співбесіди пропозицій про роботу не надходить, а конкурентна розвідка володіє потрібною інформацією. Конкурентна розвідка діє: спостерігаючи (на відстані) і (або) проникаючи в організацію (коли у фірму конкурента вводиться свій (або спеціальний) співробітник).

Методами конкурентної розвідки також є:

- опитування конкурентів, постачальників, клієнтів, колишніх співробітників;
- закупівля товару у конкурента;
- відвідування конференцій, семінарів і виставок за участю конкурентів.

Для проведення конкурентної розвідки також можна використовувати ЗТР (засоби технічної розвідки):

- апаратура радіорозвідки;
- апаратури візуально оптичної розвідки;
- лазерні мікрофони;
- закладні пристрої;
- апаратуру хімічної розвідки та інше.

Конкурентна розвідка може проводитися:

- з землі;
- з БПЛА (безпілотних літальних апаратів).

Завдання конкурентної розвідки:

- виявити конкретні недоліки в роботі конкурентів, виявити товари з конкурентними пе ревагами, визначити їх цінову політику;
- виявити способи просування таких товарів на ринок;
- виявити умови співпраці з постачальниками (щоб створити для себе умови не гірші, ніж у конкурента);
- визначити постійну клієнтську базу конкурента і умови взаємодії, визначити рівень рентабельності товарів;
- виявити плани конкурентів з технічного розвитку, розширення меж ринку.

Пропозиція щодо рішення задачі

Конкурентна розвідка особливо ефективна, коли результатом буде випередження свого конкурента, а не просто копіювання його переваг. Існує безліч способів ведення конкрентної розвідки [2]. Введемо деякі поняття, що стосуються проведення конкурентної розвідки. Отже, суб'єкт конкурентної розвідки – це підприємство, організація чи особа, що з використанням певних ресурсів здійснює збір,обробку та аналіз даних з різних джерел для вироблення управлінських рішень з метою підвищення конкурентоспроможності підприємства, організації чи своєї; об'єкт конкурентної розвідки – це підприємство, організація чи особа, до діяльність якої прикута невмотивована увага з боку іншого об'єкта, що проводить збір інформації про діяльність та стан з метою нанесення шкоди чи отримання вигоди. Слід не лише приділяти увагу проведенню конкурентної розвідки. Існує можливість, що суб'єкт конкурентної розвідки, який реалізує системну програму збору, аналізу і розподілу інформації про діяльність конкурента(-ів), в той самий час може бути об'єктом конкурентної розвідки. Повністю уникнути можливих дій конкурентів з метою отримання інформації, що становить КТ, чи будь-якої іншої, розповсюдження якої завдасть шкоди, неможливо. А отже необхідно проводити заходи, що забезпечать неможливість отримання інформації такого змісту. Одним із способів запобігання впливу конкурентної розвідки на діяльність підприємства – це розробка заходів захисту відомостей з обмеженим доступом.

При розробці заходів захисту відомостей з обмеженим доступом необхідно:

1. Одержати загальні задачі щодо захисту відомостей з обмеженим доступом (ВзОД) з керівної організації вищого рівня ієрархії, замовника.
2. Створення робочої групи для розробки заходів захисту.
3. Визначити задачі захисту на різних етапах життєвого циклу продукту, його застосуванню, технології виготовлення.
4. Аналіз ВзОД для визначених етапів життєвого циклу.
5. Виявлення та аналіз основних відомостей (ОВ).

6. Виявлення небезпечних засобів технічної розвідки ЗТР для ОВ та можливих результат тів їх діяльності.
7. Розробка замислу захисту.
8. Розробка заходів захисту.
9. Розробка заходів контролю заходів захисту.

При розробці засобів захисту першочергово необхідно визначити доцільність та конкретизувати мету проведення цих заходів: чи існує на об'єкті обробка, створення, модифікація і т.д. інформації, такої, що містить відомості з обмеженим доступом. На приватних підприємствах рішення про віднесення інформації до такої, що необхідно захищати від витоку (несанкціонованого ознайомлення і т.д), приймається керівником підприємства чи його уповноваженого (групою керівників). Етап одержання загальних задач щодо захисту є дуже важливим, оскільки саме в цей момент відбувається формування загального та детального списку ВзОД, що повинен бути отриманий у вигляді офіційно оформленого розпорядження від замовника, в якому має міститися час, термін та місце проведення відповідних робіт.

У склад робочої групи доцільно ввести:
- фахівців, які володіють знаннями щодо усього об'єкту захисту або його складових частин,
- фахівця з ЗТР,
- економіста для оцінки можливих втрат від витоку ВзОД та обґрунтовування витрат на заходи захисту ВзОД.

Визначення задач захисту на різних етапах життєвого циклу продукту, його застосування, технології виготовлення:

1. Етап теоретичних досліджень з створення об'єкту захисту.
2. Етап створення та дослідження окремих фрагментів, макетів елементів об'єкту захисту.
3. Виготовлення дослідного зразка (кількох зразків).
4. Випробування дослідного зразка повномасштабні або окремі.
5. Підготовка масового виробництва, технологій масового виробництва.
6. Масове виробництво.
7. Продаж, повномасштабне застосування, включаючи експлуатацію, ремонт тощо.
8. Утилізація.

На кожному з етапів потрібно визначати заходи захисту, які необхідно впроваджувати для забезпечення захисту ВзОД. Для певного етапу життєвого циклу необхідні заходи захисту можуть відрізнятися. Це залежить від місця етапу в життєвому циклі. Також набір етапів може змінюватися в залежності від типу та характеру об'єкту захисту.

Потрібно прогнозувати можливості модернізації об'єкту ВзОД. Це може привести до проявлення зворотного зв'язку до визначення задач захисту на різних етапах життєвого циклу продукту від більш пізніших етапів життєвого циклу. Не усі етапи життєвого циклу можуть мати місце для конкретних об'єктів захисту. Також перелік та кількість етапів життєвого циклу може відрізнятися для конкретних об'єктів захисту.

Особливості та вимоги для вирішення поставленої задачі

Суть аналізу ВзОД для визначених етапів життєвого циклу полягає у декомпозиції загального переліку ВзОД та створення набору елементарних ВзОД.

1. B – відомість з обмеженим доступом (множина); $b_1,\ b_2 \dots b_n$ – множина ЕлВзОД, що визначено для певної ВзОД;

$$\exists \forall B := \{b_1,\ b_2 \dots b_n\} \tag{1}$$

Існує всяка множина B, що рівнозначна множині $\{b_1,\ b_2 \dots b_n\}$.

2. A є множиною всіх елементів, що є ВзОД.

$$A = U \tag{2}$$

3. Кожний елемент B є елементом A «і» A не дорівнює B.

$$B \subseteq A \wedge B \neq A \tag{3}$$

4. С – множина, що містить у собі елементи – ознаки відомостей(ОВ).

$$C = \{c_1, c_2 \dots c_n\} \tag{4}$$

5. P – властивість ознаки; оприлюднення завдає шкоди.

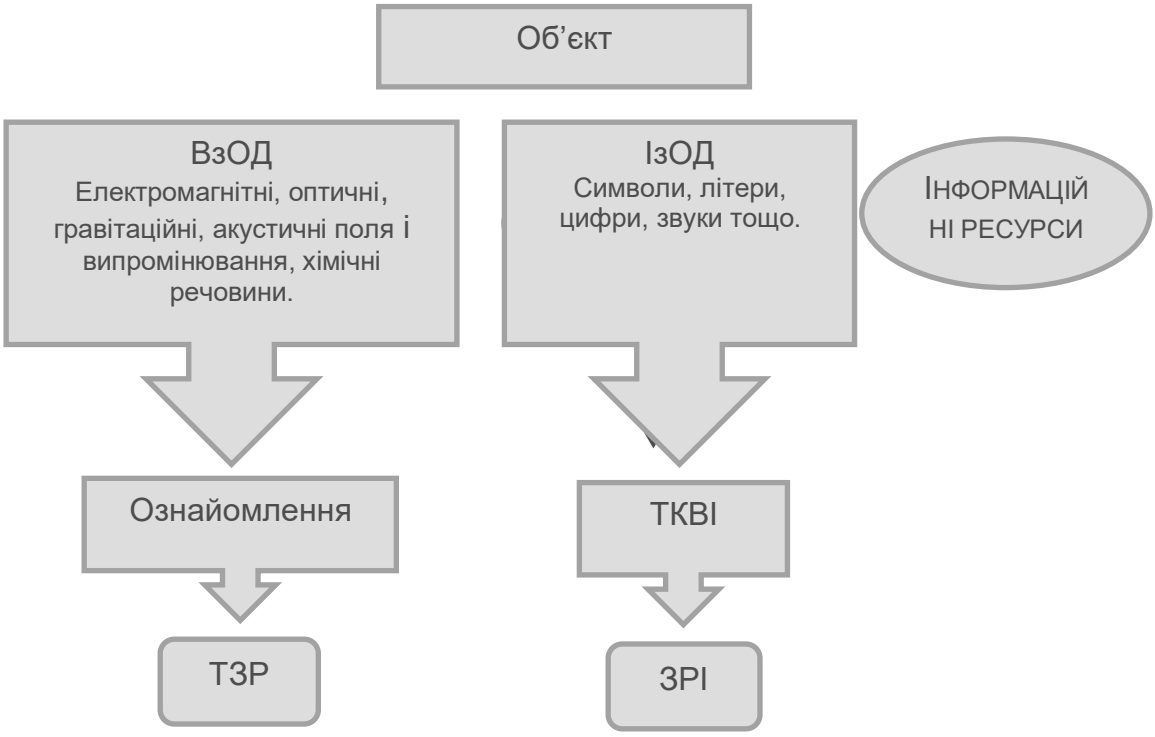
$$\exists \forall D \in \{x \in C\}: P(\{C\})\} \tag{5}$$

6. Існує множина E, що мітить відомості з інформаційних ресурсів. Серед елементів множини E не може бути елементів множини A.

$$E \cap A = \emptyset \tag{6}$$

7. Множина ЗТР – Z, елементами якої є засоби, що можна використати для отримання ІзОД по технічним каналам витоку інформації (ТКВІ), де z_n – це засоби технічної розвідки (рисунок).

$$Z \in \{z_1, z_2, z_3, \dots z_4\} \tag{7}$$



Обидва види прояву даних потребують захисту від технічних розвідок. Знакова форма представляє сукупність символів, літер, цифр, звуків, які відображають предмети та явища реального світу у віртуальному світі. Носіями інформації з обмеженим доступом (ІзОД) є

інформаційні сигнали у формі фізичних полів (електромагнітних, оптичних, акустичних), електричних сигналів, вібраційних коливань у твердих предметах. Шлях захисту від таких розвідок – технічний захист інформації (ТЗІ) [1].

Інструмент даного етапу – метод експертних оцінок, що є одинм з основних класів *методів науково-технічного прогнозування*, який ґрунтується на припущенні, що на основі думок експертів можна збудувати адекватну *модель* майбутнього розвитку об'єкта *прогнозування* та відправною інформацією при цьому є думка спеціалістів, які займаються дослідженнями й розробками в прогнозованій галузі. Робоча група проводить аналіз загальних задач захисту ВзОД для створення набору елементарних ВзОД (ЕлВзОД).

При визначенні набору ЕлВзОД необхідні:

- мета робіт та заходів, що будуть впроваджуватися;
- перелік (набір) ЕлВзОД, що повністю забезпечуватиме ВзОД;
- можливий діапазон значень ЕлВзОД;
- шкала вимірювання значень ЕлВзОД, що дозволить визначити можливі наслідки та збитки у разі розкриття конкурентами даної інформації, що становить конкретну ЕлВзОД;
- необхідна та можлива точність вимірювання значень ЕлВзОД для рішення задач конкурентної розвідки.

Етап виявлення та аналізу ОВ характерний тим, що робоча група методом експертних оцінок для кожного ЕлВзОД виявляє усі ОВ. Даний етап є найбільш відповідальним та складним. Досвід членів робочої групи є запорукою його вірної реалізації.

Коректність та вичерпність визначення ЕлВзОД може забезпечити відповідність розроблювальних та повноту заходів захисту задачам по захисту ВзОД, та з певною вірогідністю гарантувати захист ВзОД.

Вичерпність визначення ЕлВзОД забезпечується:

- розумінням призначення та мети захисту;
- коректністю та змістовністю поставлених задач по захисту;
- компетентністю та відповідно високий професійний рівеньробочої групи;
- вичерпністю переліку інформацію, захист якої необхідно забезпечити.

Виявлення небезпечних ЗТР для ОВ та можливих результатів їх діяльності, визначення відомостей, що можуть бути здобуті з використанням певного засобу технічної розвідки. Для кожної пари ОВ – ЗТР встановлюється можливість проведення розвідки – „реалізації ОВ”. Реалізація ОВ оцінюється спочатку якісно, а потім кількісно. При якісній оцінці виявляються потенційні можливості ЗТР реалізовувати ОВ. При кількісній оцінці обчислюється ймовірність реалізації ОВ. Розробка замислу захисту здійснюється методом експертних оцінок. На даному етапі методом експертних оцінок проводиться прогноз синтезу за ЗТР кожного з ЕлВзОД по набору ОВ, які реалізуються ЗТР.

Складність етапу пояснюється принциповою неоднозначністю результату синтезу по набору ОВ. Причина – набір ОВ, їх значення встановлюється імовірнісним. Тим не менш, робоча група з’ясовує яке рішення може прийняти система розвідки по одержаним розвідданим.

Якщо ОВ проявляються потужно, то краще надалі застосовувати спосіб технічної дезінформації цієї ЕлВзОД. У противному випадку – краще застосовувати спосіб приховування.

Технічна дезінформація також може стати більш дієвою у випадку, коли про існування об’єкту захисту вже відомо. У цьому випадку доцільнішим буде введення в оману конкурентів. Під «введенням в оману» слід розуміти процес надання конкуренту завідома неправдивої інформації, видаючи її за автентичну.

Не менш важливим є визначення економічної обґрунтованості розроблених заходів захисту, чи можливо після впровадження розроблених заходів захисту зберегти економічну привабливість розробки. Великі витрати на впровадження та підтримку заходів захисту

призводять до зменшення розміру чистого прибутку, через компенсування витрат на заходи захисту, що в свою чергу зменшує економічну привабливість об’єкту [4]. Повинен бути знайдений компроміс, за якого витрати на заходи захисту матимуть оптимальне поєднання гарантії безпеки від конкурентної розвідки та ціни, а витрати будуть співрозмірні із загальним бюджетом розробки та виробництва об’єкту захисту. Економічна доцільність розробленого комплексу заходів захисту повинна бути такою, що витрати на впровадження та підтримку працездатності заходів захисту не перевищуватимуть втрат від витоку інформації. Така оцінка має проводитися економістом із складу робочої групи.

Висновки

Визначено, що розробка заходів контролю заходів захисту направлена на неможливість та попередження невиконання розроблених заходів захисту для розроблюваного об’єкту. Заходи контролю необхідні для підтримки працездатності створеної системи заходів захисту.

Відображено можливість застосування апарату теорії множин для формалізації задач захисту відомостей з обмеженим доступом. Вказано на необхідність пов'язування задач захисту від конкурентної розвідки з основними етапами життєвого циклу виготовленого продукту. Методикою визначено основні цілі та завдання кожного етапу для проведення робіт. Приведена методика може використовуватися при організації заходів захисту від технічних засобів конкурентної розвідки.

Список літератури: 1.*Заболотний, В.І.*, Класифікація технічних каналів витоку інформації / В.І. Заболотний // Радіотехніка. – 2003. – Вип. 134. 2. *Воронов, Ю.П.* Конкурентна розвідка : посібник. – Новосибірськ : Вид-во Новосибір. держ. ун-ту, 2007. – С. 32. 3. *Цивільний* кодекс України, ст. 505. 2003 4. *Заболотний, В.І.* Обґрунтування вибору заходів захисту характеристик продукції від конкурентної розвідки // Прикладна радіоелектроніка. – 2013. – Т. 12. – №2. – С. 351-356.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 03.04.2017