УДК 621.39:65.012.8

В.І. ЗАБОЛОТНИЙ, канд. техн. наук, А.А. АБУЗОВА, В.І. ВОЛОБУЄВ

ОБҐРУНТУВАННЯ ПЛАНУ ЗАХИСТУ ОБ'ЄКТІВ ІНФОРМАЦІЇ ПРО ОБ'ЄКТИ, ПРОЦЕСИ ТА ЯВИЩА

Вступ

Розвиток України в економічному плані інтенсифікує процес збільшення матеріального виробництва конкурентоздатної науковоємної продукції. Отримати суттєвий прибуток від своєї продукції власник може тільки у тому випадку, коли забезпечить раптовість її появи на відповідному ринку [1]. У сфері матеріального виробництва раптовість стосується: параметрів, споживчих характеристик виробів, терміну початку, обсягів, місця виробництва, застосованих новітніх технологій. Вказані дані конкуренти спроможні одержати за допомогою методів та засобів, у тому числі і за рахунок використання відповідних технічних засобів.

Відомі два шляхи добування даних за допомогою засобів технічних розвідок [1].

По-перше, є шлях добування інформації, яка існує у знаковій формі. 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 [3] у формі фізичних полів (електромагнітних, оптичних, акустичних і електричних сигналів, вібраційних коливань у твердих предметах. Шлях захисту від таких розвідок – технічний захист інформації (ТЗІ). Національні стандарти та інші документи щодо його реалізації широко відомі [3 – 5].

По-друге, конкуренти можуть спостерігати власне за самими матеріальними об'єктами у тому числі за допомогою засобів технічних розвідок. Форма проявлення матеріальних об'єктів реального світу у процесі виробництва й застосування продукції різного призначення – електромагнітні, оптичні, гравітаційні, акустичні та інші поля й випромінювання, хімічні речовини [3]. Мова про такий шлях добування даних йдеться у ряді джерел [2, 3, 5]. Тому для забезпечення принципу раптовості з'явлення на ринку продукції необхідне забезпечення прихованості розробки, виготовлення дослідних зразків та їх повномасштабних випробувань [1]. Надалі характеристики реальних об'єктів, що проявляються ними через фізичні поля та хімічні речовини, будуть називатися відомостями з обмеженим доступом (ВзОД) для відрізнення від інформації з обмеженим доступом (ІзОД) яка підлягає технічному захисту.

На даний час з'являються роботи про заходи захисту ВзОД як захист від конкурентної розвідки у бізнесі [6]. Планування таких заходів потребує певної формалізації процесів розвідки-захисту для прийняття рішень у цій сфері.

Одним із способів формалізації процесів розвідки-захисту є застосування математичного апарату логічних систем розпізнавання об'єктів та явищ [7]. Причому там наведено підходи впливу маскування та протидії розвідці на якість розпізнавання.

Недоліками запропонованих підходів є, по-перше, визначені фіксовані образи об'єктів, що підлягають захисту і об'єкти, під які здійснюється маскування. Цим самим обмежується можливість захисту технічних характеристик нової продукції від конкурентної розвідки, що у ряді випадків є визначальним. По-друге, логічні системи розпізнавання орієнтовані більше на якісний опис образів об'єктів, чим на кількісний, що затрудняє їх використання.

Подоланню цих недоліків і призначена стаття.

Постановка задачі

Нехай підприємство (розробник) підійшло до виготовлення експериментального зразка і випробування нового виробу. Новий виріб відноситься до певного типу групи виробів, де K – кількість типів виробів даної групи. Вироби випускають на різних підприємствах, які можуть знаходитися у конкурентних відносинах.

Перелік типових характеристик виробів групи відомий. Їх кількість M. Окремі або усі характеристики нового виробу представляють собою ВзОД (табл. 1). Обмеження доступу до ВзОД – до часу вільного продажу нового виробу.

Таблиця 1

Характеристики виробів	Вироби					
	Існуючі K типів					Новий
	B_1	...	$B_к$	...	B_K	B_H
$П_1$	$П_{11}$	...	$П_{1к}$	...	$П_{1K}$	$П_{1H}$
$П_2$	$П_{21}$	...	$П_{2к}$	...	$П_{2K}$	$П_{2H}$
...	...	...	...	...	...	...
$П_м$	$П_{м1}$	...	$П_{мк}$	...	$П_{мK}$	$П_{мH}$
...	...	...	...	...	...	...
$П_M$	$П_{M1}$	...	$П_{Mк}$	...	$П_{MK}$	$П_{MH}$

Задача – спланувати діяльність по захисту ВзОД від конкурентів щодо основних характеристик виробів до часу зняття обмежень на ВзОД.

Способи захисту [3 – 8] ВзОД: дезинформація та (або) приховування.

Дезинформація, виходячи із задуму, може спрямовуватися до нав'язування конкурентам відомостей про споживчі характеристики виробів:

1) погіршених;

2) завищених.

Приховування спрямоване на забезпечення невизначеності конкретних характеристик конкурентами за результатами ведення розвідки.

За результатами розвідки конкуренти можуть приймати певні рішення (табл. 2).

Таблиця 2

Спосіб захисту ВзОД	Реакція конкурента на одержані відомості	Дії конкурента на подальшу розвідку
Дезинформація на погіршення характеристик	Довіра	Відмова
	Недовіра	**Посилення**
Дезинформація на завищення характеристик	Довіра	Відмова
	Недовіра	**Посилення**
Приховування	Продовжувати розвідку	**Посилення**

Довіра конкурентів до результатів розвідки може базуватися на невеликому відхиленні одержаних ВзОД від очікуваних, типових для даної групи виробів. Відсутність даних про споживчі характеристики виробу буде вести до посилення розвідки.

Посилення розвідки є негативним результатом заходів захисту. Це може привести до додаткових витрат на заходи захисту і обмежень у ході виготовлення та випробувань виробу.

З викладеного витікає необхідність зваженості обґрунтування та проведення заходів дезинформації при припустимих заходах приховування.

Зваженість обґрунтування повинна витікати з кількісних показників, які будуть наведені далі.

Пропозиція щодо рішення задачі

Суть пропозиції заключається у оцінці припустимого значення кожної характеристики нового виробу, що підлягає захисту способом дезинформації, як випадкової величини на тлі відомих подібних характеристик даної групи виробів. Випадковість характеристики для розвідки грунтується на її апріорній невідомості для конкурента. У ході розвідки набираються розвіддані і по них поступово можуть уточнюватися конкретні значення характеристик.

Хибні розвіддані або їх недостатність, створені заходами дезинформації і приховування, приведуть до хибних оцінок.

Таким чином, апріорний розподіл кожної із характеристик може бути визначений типовими, відомими значеннями $П_м\{П_{м1}, ..., П_{мк}, ..., П_{мК}\}$. Відомі величини $П_{мк}$ можна представити як багатокутник частот з нерівномірним поділом по вісі абсцис. Значення окремих характеристик $П_{мк}$ можуть бути як дискретними, так і безперервними у певному діапазоні.

Апріорні ймовірності схожості характеристик нового виробу під старі $p(B_к)$ можна узяти рівними, якщо інших даних про це немає. У такому випадку, з точки зору теорії інформації, невизначеність розподілу характеристик в інтервалі області визначення буде найбільша.

З початку розвідки апостеріорні характеристики розвідуваного параметру будуть стягуватися до такого значення, до якого будуть приводити розвіддані.

Ще раз слід зазначити, що науково-технічний прогрес, за своїм змістом, спрямований на поліпшення споживчих характеристик виробів. Поліпшення не обов'язкове для усіх характеристик, деякі другорядні характеристики можуть і погіршуватися. Тому при розробці заходів захисту можна використовувати дане положення і дезінформовувати відносно визначеного набору характеристик як у погіршення, так і поліпшення характеристик. Процес обрання згаданих характеристик у роботі не розглядається. Він може бути встановлений експертною групою розробника, виходячи із конкретної природи характеристики виробу.

Для кожної характеристики слід встановити ранг, за яким визначається пріоритет важливості захисту.

Деякі характеристики функціонально пов'язані між собою і між ними існує зв'язок. Такий зв'язок може встановлюватися методами регресійного аналізу. Окремими випадками регресійного аналізу може бути кореляційний аналіз. Кількість парних регресій, що потрібно визначити, буде $M!/(2 \times (M - 2)!)$ співвідношень, що при застосуванні комп'ютерної техніки нескладно виконати.

Для залежних пар характеристик ранг може складатися як сума рангів відповідних вихідних рангів характеристик.

Експертна група, також повинна встановити напрям зміни величини характеристики по вісі шкали у сторону їх погіршення та завищення.

Оцінку якості заходів захисту по кожній характеристиці для нового виробу можна проводити шляхом співставлення очікуваного результату захисту із густиною розподілу значення відповідної характеристики для множини типів виробів. Недоліком використання співставлення розподілів випадкових величин є складність визначення законів їх розподілу із-за невеликої вибірки типів виробів – K. Зазначений недолік можна подолати за рахунок використання моментів випадкових величин: 1) математичного очікування, 2) середньоквадратичного відхилення; нормованих центральних моментів 3) третього порядку (асиметрія) та 4 четвертого порядку (ексцес).

Співставлення значення характеристики нового виробу з 1) та 2) параметрами дає уяву про величину її споживчої якості на відповідній шкалі.

Асиметрія та ексцес свідчать про тенденції групування значень характеристик виробів. Для від'ємної асиметрії – переважає велика густина характеристик із великим значеннями над малою густиною менших величин і навпаки. Позитивний ексцес свідчить про гостровершинну скупченість значень характеристик, а від'ємний – про плоску вершинну. Означені моменти 3) та 4) можуть обгрунтовувати доцільність вибору для дезинформації конкретних значень характеристик на тлі відомих.

Розробка плану захисту – вибору значень характеристик для дезинформації конкурента повинна відповідати певним принципам [5].

Комплексності захисту – у перекритті усіх нетехнічних і технічних каналів витоку інформації по фізичним полям. Всі заходи щодо захисту повинні бути узгодженні за місцем, метою і часом.

Активності захисту – у наполегливому нав'язуванні конкуренту невірної інформації про приховуваний виріб.

Переконливості захисту – у правдоподібності, відповідати обстановці в цілому.

Безперервності захисту – у постійному проведенню, у будь-яких умовах, за будь-яких обставин у процесі заданого терміну часу (до рекламної кампанії, продажу).

Різноманітності прийомів захисту – виключення будь-якого шаблону і формальності при проведенні захисту.

Заходи захисту також повинні бути економічно обгрунтованими.

Алгоритм рішення задачі

1. Складається опис відомих виробів у формі табл. 1. Додається стовпчик із конкретними характеристиками для нового виробу, які можуть складати як ВзОД, так і відкриті дані.

2. Експертна група проводить ранжування конкретних характеристик нового виробу по ступеню важливості по їх захисту від конкурентів.

3. Обчислюють математичне очікування, середньоквадратичне відхилення, асиметрію та ексцес усіх технічних характеристик виробів.

4. Методом найменших квадратів оцінюються коефіцієнти парної регресії для усіх можливих пар характеристик $П_i П_м$. Встановлюються ранги для пар характеристик.

5. Згідно одержаного рангу для одиночних характеристик, починаючи з найвищого, експертами пропонуються заходи захисту щодо споживчих характеристик виробів:

– із погіршенням характеристик високих рангів (дезинформація);

– приховуванням та погіршенням характеристик середніх рангів;

– покращенням характеристик низьких рангів (дезинформація).

6. Провести перевірку на узгодженість заходів захисту характеристик низьких рангів заходам захисту характеристик високих рангів по коефіцієнтам парної регресії (п.4) і відповідним чином їх відкоригувати (п.5).

7. Скласти сукупний опис відомих виробів і нового виробу з характеристиками, що пропонується показувати конкурентам, у формі табл. 1 (змінений останній стовпчик ВзОД на характеристики які потрібно пред'являти конкурентам).

8. Визначити ознаки ВзОД, які треба захищати способами дезинформації і приховування. Перевірити можливість реалізації запропонованих заходів при виготовленні та випробуваннях нових виробів. При неможливості – повторити дослідження, починаючи з п. 5. І так до досягнення бажаного результату.

9. Скласти план заходів дезинформації і приховування від конкурентної розвідки за розділами:

– заходи дезінформації у відкритих джерелах інформації, Інтернеті тощо;

– заходи забезпечення контрольованої зони навколо об'єктів з виготовлення та випробування нових виробів;

– заходи захисту від безпосереднього спостереження та технічної розвідки за виготовленням і випробуванням виробів із-за меж контрольованої зони способами технічної дезінформації та приховування.

Даний алгоритм дає основу для обґрунтованої розробки комплексу захисту нових виробів від конкурентної розвідки.

Рішення даної задачі доцільно проводити на ПОЕМ із використанням програмного забезпечення обробки статистичних даних.

Висновки

Формалізація задач захисту дозволяє розробляти їх варіанти, порівнювати між собою та обирати кращі з них по визначеним критеріям.

Застосування обчислювальної техніки з програмним забезпеченням із статистичних розрахунків полегшує та прискорює дослідження варіантів захисту.

Список літератури: 1. *Заболотний В.І.* Класифікація технічних каналів витоку інформації // Радіотехніка. – 2003. – Вип. 134. 2. *Ющук Е.А.* Конкурентная разведка: маркетинг рисков и возможностей. – Казань : Экспресс-формат, 2010. – 241 с. 3. *ДСТУ3396.2-97* Захист інформації. Технічний захист інформації. Терміни та визначення. 4. *ДСТУ3396.0-96* Захист інформації. Технічний захист інформації. Основні положення. 5. *Положення* про технічний захист інформації в Україні. Затверджено постановою КМУ 9 вересня 1994 р. №632 // Збірка нормативних документів системи технічного захисту інформації, 1997. 6. *Кузин А.А., Нежданов И.В., Ющук Е.А.* Дезинформация и активные средства в бизнесе. – Казань : Яналиф, 2009. – 134с. 7. *Горелик А.Л., Скрипкин В.А.* Методы распознавания. – М. : Высш. шк., 1984. – 208 с. 8. *Брусницын Н.А.* Информационная война и безопасность. – М. : Вита-Пресс, 2001. – 280 с.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 17.07.2011