8. Вишневский Ю.. Что останется от среднего класса // Комментарии. – 2009. – №2(156).
9. Human Development Report, 1997. – NEW YORK: UNDP, 1997. – P. 5. (40).
10. Гончаров Ю. В., Щербина І. В. Підвищення питомої ваги та ролі середнього класу в структурі населення України: передумови, проблеми, перспективи / Препринт наукової доповіді. – К.: ТОВ «Дорадо-Друк», 2010. – 66 с.

Надійшла 09.07.2010

УДК 338.24

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ВІД ПРОМИСЛОВОГО ШПІОНАЖУ

Н.О. БАБІНА

Київський національний університет технологій та дизайну

Стаття присвячена актуальній проблемі визначення основних технологій захисту комерційної таємниці сучасного підприємства (фірми). На основі аналізу промислового шпигунства, його основних методів визначені джерела витоку комерційної таємниці і сформульовані організаційні, адміністративні та соціально-психологічні засоби захисту секретної інформації від недобросовісних конкурентів

Людство завжди цікавилося чужими таємницями і давно вже збагнуло, що інформація коштує дуже дорого. Потягом тисячоліть носієм та джерелом передачі інформації виступала людина. З виникненням писемності папір на роки став єдиним хоронителем таємниць. Розвиток науково-технічного прогресу сприяв вдосконаленню розмірів та технічних характеристик приладів, що дозволяли таємно отримувати, фіксувати та надійно захищати інформацію.

Тривалий період основним замовником інформації про своїх опонентів виступала держава. З часом, великі промислові корпорації, які тісно переплелися з державою, почали використовували дані військової розвідки для своїх приватних цілей, закладаючи, тим самим підвалини промислового шпигунства. Помірній ціні і нескладність у використанні в наш час призвели до того, що технічні засоби отримання інформації стали доступні достатньо широкому колу користувачів.

За часів існування СРСР поняття промислового чи економічного шпигунства майже не вживалося у пресі чи науковій літературі, відкритій для широкого загалу, а термін «комерційна таємниця підприємства» використовувався по відношенню до іноземних господарюючих суб'єктів.

Сучасні фахівці у галузі економічної безпеки виділяють певні етапи у розвитку промислового шпіонажу. Перший етап пов'язаний зі становленням бізнесу в країні, з зародженням підприємств різної форми власності та конкуренції. В цей період економічна безпека залишалася прерогативою держави. Окремі підприємці збирали інформацію про конкурентів несистематично та не професійно. Другий етап співпадає з формуванням незалежних держав на тлі СРСР, розпадом спецслужб, виходом підприємств на зарубіжні ринки. Спеціальна апаратура служб держбезпеки почала з'являтися у приватних осіб. Третій етап пов'язаний зі становленням ринкової економіки, розвитком підприємництва, створення великої кількості підприємств різної форми власності. На цьому етапі виникає велика кількість приватних охоронних і детективних агентств, в більшості кадрово сформованих із професіоналів, які залишили службу в органах безпеки. Виробництво теж швидко опанувало нову галузь: конверсія

оборонних підприємств призвела до того, що вітчизняні вироби не тільки конкурували із західними аналогами, але й перевершували їх за якістю і ціною.

Інтернет і багато чисельні спеціалізовані виставки дозволяють краще орієнтуватися у спеціальній продукції, яка використовується як з метою захисту і охорони, так і для доступу для комерційної таємниці конкурентів.

Сьогодні протистояти промисловому шпигунству стає дедалі складніше: підвищився рівень підготовки «розвідників», які озброєні сучасною технікою; законодавство не повністю адаптоване до сучасного етапу розвитку суспільства; кількість фахівців з промислового шпигунства не може задовольнити потреби ринку; сучасні бізнесмени слабо обізнані в тому, що таке аналітична робота, економічна розвідка та ін З іншого боку, кримінальний світ швидко прогресує і професійно протистоїть «чистому» бізнесу, в сфері отримання корисної інформації зокрема.

Це істотно підвищує ступень загроз економічній безпеці підприємств, ефективна підтримка якої можлива тільки в разі створення на підприємстві стабільної системи захисту від зовнішніх та внутрішніх небезпек.

Об'єкти та методи дослідження

Різні аспекти економічної безпеки підприємств в ринковій економіці розглядалися в працях вітчизняних та зарубіжних вчених-економістів. Так, економічна безпека України в умовах ринкових трансформаційних процесів, генеза її становлення є предметом вивчення В.Богачова, Н.Вавдіюк, Т.Сухорукової, В.Ткаченка. Питання економічної безпеки підприємства: захист комерційної таємниці, діагностика рівня економічної безпеки підприємства, чинники інформаційної безпеки підприємства, юридичні аспекти безпеки підприємства є предметом дослідження таких вчених, як Г.Андрощук, С. Довбня, М.Живко, Г.Козаченко, П. Крайнєв, В.Хорошок.

Проблема створення сучасної системи захисту від промислового шпигунства досліджується А.Бердинським, С.Гіріним, А.Лисовим, Т.Ткачуком та ін. В. Єгоров вивчає історію розвитку промислового шпигунства [1], М.Денюзьєр досліджує методи конкурентної розвідки і промислового шпіонажу. Особливостям економічного шпигунства, конкурентній розвідці і контррозвідці присвячені праці І.Березина та О.Івченка.

Однак необхідно зазначити, що у вітчизняній і зарубіжній літературі дотепер не знайшли належного відображення деякі важливі аспекти економічної безпеки підприємств: значної уваги заслуговує питання виявлення особливостей промислового шпигунства в умовах нестабільності і підвищення ризиків та створення надійної системи захисту сучасного підприємства.

Постановка завдання

Основна мета дослідження – на основі аналізу промислового шпигунства, його основних методів виявити можливі джерела розголошення комерційної таємниці підприємства (фірми) і сформулювати організаційні, адміністративні та соціально-психологічні засоби захисту секретної інформації від недобросовісних конкурентів.

Результати та їх обговорення

Поняття «шпигунство» означає одержання або добування відомостей, що становлять певний інтерес. Промислове шпигунство - це різновид економічного шпигунства, метою якого є одержання

інформація про діяльність одного або декількох підприємств-конкурентів. Суб'єктом економічного шпигунства є окремий промисловець, підприємство, фірма, тобто фізична або юридична особа.

Фахівці визначають промислове шпигунство як вид недобросовісної конкуренції, діяльність із незаконного добування відомостей, що становлять комерційну цінність. [2,18]. Для підприємництва промислове шпигунство виступає способом конкурентної боротьби, метою якої є: з одного боку, отримання конфіденційної інформації про стратегічні й тактичні наміри бізнесу конкурентів; з іншого - здобуття конкурентної переваги на ринку, через витіснення або знищення суперника.

Промислове шпигунство необхідно відрізняти від конкурентної розвідки. Термін «конкурентна розвідка» (competitive intelligence) широко використовується західними фахівцями безпеки бізнесу і означає дослідження відкритих інформаційних джерел про основні тенденцій бізнесу й наміри конкурентів, аналіз ризиків та вразливих місць суперників.[3, 19]. Головною відмінністю між конкурентною розвідкою та промисловим шпигунством є методи й способи отримання інформації: розвідник діє в правовому полі, не порушує норм законів (хоча його дії не завжди відповідають морально-етичним нормам ведення чесної конкурентної боротьби); промисловий шпіонаж передбачає і нелегальні методи й технології.

В промисловому шпигунстві використовують агентурні методи і технічні методи.[3, 21]. Агентурний метод одержання інформації є основою будь-якого виду шпигунства. Найбільш уживаними є два напрями діяльності: вербування і «впровадження» своєї людини. До технічних методів відносяться: встановлення відповідної апаратури для прослуховування в офісах та приміщеннях, «закладки» по лінії телефонного кабелю, «мобільне шпигунство» та ін. [4, 24].

Збереження комерційної таємниці – один із вагомих факторів забезпечення економічної безпеки підприємства. На підприємстві повинна бути встановлена система, яка забезпечує передачу конкретним особам тільки такого обсягу інформації, який дозволяє їм сумлінно виконувати свої службові обов'язки і знижує рівень можливих збитків при переході працівника до фірми-конкурента.

З особами, які мають допуск до комерційної таємниці, необхідно постійно працювати і перевіряти їх, оскільки за даними фахівців вірогідність порушення комерційної таємниці складає: 43% при підкупі, шантажі, комерційному шпіонажі; 24% - при спілкуванні. 18% - при незаконному проникненні в комп'ютерну мережу підприємства; 10% - при викраденні документації; 5% - при прослуховуванні телефонних розмов.

За даними експертів з безпеки сприятливими умовами для декодування комерційної таємниці є: балакучість співробітників (часто в дружніх компаніях, де вживається алкоголь) – 32%; прагнення співробітників підзаробити – 24%; відсутність на підприємств служби безпеки – 14%; радянська звичка ділитися «передовим досвідом», роздавати всім поради – 12%; безконтрольне використання інформаційних та копіювальних засобів – 10%; психологічні конфлікти між співробітниками, між керівництвом і підлеглими, неправильний кадровий підбір – 8%. [5].

Найбільш типовими методами комерційного шпіонажу є підкуп та влаштування «своїх» людей до складу персоналу підприємства-конкурента.

Підкуп є самим простим і ефективним способом одержання комерційної таємниці. Безперечно, він потребує певної попередньої аналітичної роботи для з'ясування степені обізнаності співробітників

підприємства і їх долученості до комерційної таємниці. Для підкупу необхідно точно знати: кому давати гроші, скільки, коли, через кого і за що. Всі витрати на сбір такої інформації перекриваються однією важливою обставиною – співробітнику не потрібно долати фізичні та технічні перепони для проникнення в секрети підприємства. Тому метою «розвідника» стає пошук носіїв необхідної інформації, які незадоволені своїм заробітком, кар'єрним зростанням, характером відносин з керівництвом, тих, хто гостро потребує грошей та ін.

За даними статистики Інтерполу 25% службовців готові продати секрети свого підприємства в будь-який час і кому завгодно; 50;% ідуть на це в залежності від обставин; 25% є патріотами свого підприємства чи фірми. Серед 50% співробітників, які погоджуються на співробітництво з конкурентами в залежності від обставин, значна частина складає тих, кого шантажують. [5]. Виділяють шантаж двох видів. У першому випадку людину ловлять на «гачок», погрожуючи оприлюднити компромат, у другому – погрожують діями фізичного впливу (спалити будинок, викрасти дитину т а ін.)

Ще одним методом комерційного шпіонажу є влаштування «своїх» людей до складу персоналу підприємства-конкурента.

Існує два шляхи кооптування агента у склад персоналу: перший - він працює за спеціальністю під своїм прізвищем; другий – працевлаштування здійснюється за підробленими документами під прикриттям «легенди». Ці методи більш складні, ніж підкуп і шантаж, але на відміну від завербованих інформаторів, свій агент є більш надійним і ефективним як джерело комерційної таємниці. Співпраця з таким інформатором базується на конспіративній основі: зустрічі з ним маскуються під побутові контакти, відбуваються на конспіративних квартирах або в громадських місцях, зв'язок здійснюється через «схованки», нерідко за допомогою технічних засобів. Вибіркове, таємне спостереження за співробітниками може дати керівництву підприємства цікаві факти для міркування.

Необхідно підкреслити, що невірно зосереджувати увагу тільки на тих співробітниках, які допущені до комерційної таємниці. Треба враховувати, що особа, недопущена до комерційної таємниці, може також суттєво допомогти конкурентам в проведенні комерційного шпіонажу: зробити закладку устроїв для прослуховування, виготовити копії документів, що містять комерційну таємницю, забезпечити незаконне проникнення в закриті службові приміщення, зібрати необхідні реляції про особисті і ділові якості певної особи, допущеної до комерційної таємниці.

Значною проблемою є переманювання конкурентами провідних спеціалістів фірми, оскільки це не тільки розголошення комерційної таємниці, але й ослаблення фірми на користь конкурентам. Саме тому організаційні і адміністративні засоби захисту комерційної таємниці необхідно підсилювати соціально-психологічними.

Серед соціально-психологічних засобів захисту можна виділити два основних напрями: правильній відбір і розстановка кадрів та застосування матеріальних і моральних стимулів.

Зазначимо, що відбір кадрів – генеральний напрям діяльності відділу управління персоналом, оскільки від кваліфікації, відповідальності і зацікавленості працівників прямо залежить майбутнє фірми чи підприємства. Відбір працівника на конкретну посаду починається з виявлення психологічних характеристик кандидата, що відповідають вимогам робочого місця. Потім створюється портрет ідеального співробітника, характеристики якого повністю відповідають вимогам робочого місця і

відбирається такий претендент, який буде працювати з максимальною віддачею і відчувати себе комфортно на даній роботі. Після аналізу робочого місця і відбору претендентів, здійснюється відбір майбутніх працівників. Критерії відбору зазвичай встановлює менеджер відповідного профілю.

Найбільш загальними для працівників виробництва є наступні:

- освіта (при рівних показниках перевага віддається більшому рівню освіти і її відповідності конкретній праці);
- досвід (оскільки роботодавці часто ототожнюють досвід з можливостями працівника, одним із способів вимірювання досвіду роботи є встановленні рейтингу трудового стажу);
- фізичні та медичні показники (для робіт, що потребують фізичної витривалості, сили);
- соціальний статус (так, деякі роботодавці віддають перевагу одруженим працівникам);
- персональна характеристика,
- психологічний тип особистості.

Висновки

Активізація промислового шпигунства істотно підвищує ступень загроз економічній безпеці підприємств. Тому в умовах збільшення ризиків на одне з перших місць в підприємницькій діяльності виходить проблема захисту комерційної таємниці.

В результаті проведеного дослідження встановлено, що промислове шпигунство як вид недобросовісної конкуренції, виступає способом конкурентної боротьби, основною метою якої є отримання конфіденційної інформації про конкурентів для здобуття конкурентної переваги на ринку або знищення суперника. Промислове шпигунство необхідно відрізняти від конкурентної розвідки, оскільки у них різні методи й способи отримання інформації. Основними методами промислового шпигунства є агентурні і технічні методи. Найбільш типовими агентурними методами комерційного шпіонажу є підкуп та влаштування «своїх» людей до складу персоналу підприємства-конкурента.

Для запобігання розголошення комерційної таємниці організаційні і адміністративні засоби захисту комерційної таємниці необхідно підсилювати соціально-психологічними.

Правильний підбір і розстановка кадрів дозволяє підприємствам зменшити ризики розголошення комерційної таємниці та гідно протистояти промисловому шпигунству.

ЛІТЕРАТУРА:

1. Єгоров В. З історії розвитку промислового шпигунства // Дзеркало тижня. – 1994. – 31 грудня. – № 13. – с. 14 -17.

2. Демидов Б., Величко А., Волощук И. Тайный фронт // Національна безпека України. – 2005. – № 7–8. – с. 17–23.

3. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка // Юридичний журнал. – 2003. – № 7.

4. Березин І. Промислове шпигунство, конкурентна розвідка, бенчмаркинг й етика цивілізованого бізнесу // Практичний Маркетинг. – 2005. -- 22 липня. – № 101.

5. Ревак І.О., Живко З.Б. Економічні чинники визначення збитків від витоку інформації //Сучасні інформаційні комунікаційні технології: Збірник тез. – К.: ДУІКТ, 2008. – с. 144–146.

Надійшла 30.06.2010