

# Олег Чор: «Характер економіки диктує те, що треба захищати»

Конкуренція, поза сумнівом, є найпотужнішим рушієм економіки. Однак недобросовісної конкуренції ця фраза аж ніяк не стосується.

Кожна успішна компанія має свої секрети. Це якісь нові технології, бази даних, плани розвитку бізнесу і т.д. Це те що надає компанії конкурентних переваг. Проте, якщо конкурент у якийсь спосіб дізнається про ваші козирі, переваги з'являться у нього, і йому вже нічого не вартуватиме використати проти вас ваші ж секрети. Тому від того, як ви вмісте оберігати свої таємниці, залежить ваша доля на ринку.

Про це «Агробізнесу Сьогодні» розповідає віце-президент міжнародного охоронного холдингу «Групи Сек'юриті» (Канада) Олег Чор.

Промисловий шпionаж в Україні: міф чи реальність? Наскільки актуальною є проблема і на яких рівнях?

Промислове шпionажство (ПШ) виникло ще з того моменту, як з'явилося поняття об'єднання людей. Племена вже тоді намагалися вкрасти одне в одного технології видобутку вогню, полювання, приготування їжі. Відтак, першими промисловими шпionагами були ще первісні люди.

ПШ можна розглядати на декількох рівнях. На міждержавному крадуть технології, необхідні для національної економіки та безпеки. На міжкордонній йдеться про крадіжку секретів у конкурентів, які займаються випуском аналогічної продукції. Проте сьогодні в умовах транснаціональних корпорацій ПН перестав бути національним явищем і на брав міжнародного розмаху.

ПШ в Україні – це безумовно, реальність. Якби це було не так, великі корпоративні структури не витрачали б на власну безпеку шалені гроші. Найпростіший приклад ПШ – це спроба вкрасти інформацію, отримати доступ до клієнтської бази конкурентів, здобути перелік цін на послуги



або отримати інформацію про ціни конкурентів напередодні тендеру.

Проте тут треба чітко розмежувати легальний і нелегальний аспекти. Найбільш розповсюджений спосіб отримати інформацію – зателефонувати конкуренту і, представившись потенційним клієнтом, випитати повний перелік послуг і цін. Це вважається легальним збір інформації, при цьому ви нічого не порушуєте. Нелегальний же, коли ви намагася отримати інформацію закритого типу, – наприклад, базу і ціни, за якими вони працюють з клієнтами, заплативши комусь зі співробітників конкурентів або взагалі використавши для цього технічні засоби, що є абсолютно незаконним і неприпустимим комп'ютерні мережі, прослуховування офісу, крадіжки документів, що містять комерційну таємницю.

Треба зазначити, що ще із радянських часів у нас побу-

тує традиція ділити професіоналів на дві категорії – «іх шпionажів\* і «наших розвідників». Звідси під шпionажством розуміється щось негативне. Я б так не поділяв. Тут доцільнішим є інший поділ – законно і незаконно. У Канаді так с – не порушуй. Навіть у контрактах прописана заборона на роботу у конкурентів протягом певного часу після звільнення. В Україні певне законодавство нібито теж є, однак особливості Канади с те, що там законодавство працює. Порушника можуть засудити, все відібрати, залишити на вулиці зі знищеною репутацією. На пострадянському просторі більш ефективним с метод 90-х – вивіз у ліс. Таку методологію захисту комерційних інтересів не хочеться навіть обговорювати.

Чи можна сказати, ідо для якихось ринків промисловий шпionаж є більш характерним, а для деяких – менш?

Я не думаю, що це може бути пов'язано зі сферою діяльності. Приміром, якщо говорити про виробництво, то навряд чи існують глобальні секрети технології випічки хліба або виготовлення ковбаси в Україні. У всякому разі я не володію інформацією, коли один молокозавод намагася вкрасти певні секрети виробництва в іншого молокозаводу. Проте не виключено, що викрадення промислових технологічних секретів можливе в галузях високотехнологічного виробництва. Але в тій сфері, де проходять тендерні закупівлі товарів і послуг, спроби отримати інформацію про пропозиції учасників тендеру легальним чи нелегальним шляхом носять широкий характер. З іншого боку, такою ж хворобою у нас є проведення тендерів, переможець яких відомий заздалегідь. Чесних торгів буває дуже мало. Або тендерні умови «підганяють» під конкретного переможця. А коли цього немає, основне – збір інформації.

Що крадуть промислові шпionаги в Україні? Яка інформація є найбільш затребуваною?

В основному, як я вже згадував, це – ціни тендерів, ціни для роботи з «особливими» клієнтами, бази для переманювання клієнтів не за рахунок якості, а за рахунок ціни...

На жаль, Україна не с країною, де масово розробляються ноу-хау. Тож вітчизняної електроніки, космічних технологій і т.д. промисловий шпionаж стосується можливо меншою мірою. У нас немає таких компаній, як Дженерал Моторз, Форд тощо. Ми торгуємо сировиною. Відтак, характер економіки диктує те, що треба захищати – своїх клієнтів, свій ринок, ціни. Разом з тям, де є виробництво, секрети його мають ретельно оберігатись.

Робота з персоналом. Як убезпечитись від витоку цінної інформації від своїх?

На мою думку, лише комплексний підхід може дава

ти результат. Це має бути система – від моменту прийому на роботу до вчасної виплати зарплатні. Треба враховувати цілу низку різних нюансів. Приміром, далеко не для всіх гроші є основним мотиватором. Для когось це може бути, наприклад, влада або страх.

Наша компанія приміром розробила цілий комплекс заходів, з допомогою котрого можна захиститися від промислового шпигунства. Якщо говорити про базовий комплект, то тут кілька основних кроків. Щонайперше – правильний підбір, виявлення людей, котрі здатні есе продавати. По-друге, постійна і системна робота з персоналом: чітке розмежування рівня доступу залежно від робочих потреб кожного співробітника, чітко складені і контрольовані інструкції – що можна і чого не можна, включаючи порядок зберігання та доступ до документів і інформації, доступ до кабінетів перших осіб компанії. До цього додається цілий комплекс заходів профілактичного характеру, які розробляються для конкретного підприємства з урахуванням його спеціалізації.

Розкажіть, будь-ласка, про профілактику промислового шпигунства з допомогою технічних засобів.

З технічних засобів – це контроль комп'ютерів. Що в цю мить співробітник друкує, над чим працює? Іноді збиток може завдати звичайна бездіяльність. Далі – контроль комп'ютерних мереж, відеоспостереження. Доступ співробітників в офіс у неробочі дні має бути регламентований. Що ж такого він там робить, що в вихідні треба приходити? Наскільки це визначено економічною доцільністю? Чи погрібно попрацювати над чимось таким, щоб інші не бачили?

Доступ до особових справ персоналу – обмежений. Що до поліграфу – можливо, але... Черновецький начебто перевіряв на поліграфі сам і перевіряв усю мерію Києва – і що з того?

Як діють промислові шпигуни? Розкажіть, будь ласка, про найбільш типові схеми, пов'язані з власним персоналом компанії.

Як це виглядає? На момент прийому працівника на роботу треба точно зрозуміти пси-



хологічний портрет кандидата, а не лише рівень його кваліфікації. І йдеться не тільки про психологічні тести. Та ж трудова книжка може вам чимало розповісти, зокрема, кількість місць праці цієї особи і причини їх зміни. Свого часу в спецслужбах було таке поняття, як схильність людини до зради. У кожної людини є своя межа стосовно того, то

### Довідка \_\_\_\_\_

Міжнародна охоронна агенція «Group-1» працює у галузі безпеки більше 20 років. Компанія спеціалізується на наданні повного комплексу послуг з організації безпеки об'єктів різної категорії складності, включаючи пожежну безпеку «під ключ» (сигналізація, пожежогасіння, димовидалення, пультовий моніторинг). Холдинг «Group-1» також працює у Канаді, Великобританії, Австралії, Азербайджані. На сьогодні «Group-1» має більш ніж 800 клієнтів в Україні, серед яких: Академія наук України, банк «Надра», компанія «Агро-Союз». Броварський казенний завод порошкової металургії, Гедеон Піхтер. Brocard.Watsons (ДІІ), ibis hotel Kyiv (ACCOR) та інші.

можна собі дозволити і чого собі дозволяти не варто. Від так, дуже важливо виявити цю межу конкретної людини ще на етапі прийому на роботу. Є люди, які апіорі працюють виключно на себе. Вони, можливо, й не чули про Макіавеллі, однак свято сповідують принцип: «Всі засоби, які служать меті – допустимі». Якщо кінцевою метою є самозбагачення за будь-яку ціну, то треба замислитися над рівнем допуску, не зважаючи навіть на високі професійні якості. А надалі – контроль його роботи.

Якщо говорити про мотив влади, то, вважаю, що кваліфікований спеціаліст цілком здатний це визначити. Чи небезпечно це? Певною мірою, так, якщо амбіції людини збудовані на комплексах. Свого часу проводились аналізи психологічних портретів членів терористичних організацій, починаючи з епохи народодовольців (XIX ст.). Дуже часто люди, котрі не змогли самореалізуватися у якійсь сфері, намагалися реалізуватися у такий спосіб. Вбивця Джона Леннона був саме таким. Комплекси Гітлера базувались на тому, що його не визнали свого часу як художника, а В. Ульянова – на тому, що як юрист він не виграв

в суді жодної справи. А першим відомим в історії став Герострат, котрий не спромігшись щось створити, вирішив прославитися тим, що спалив храм Артеміди. Людина такого типу, яка не здатна забезпечити високі продажі, може самоствердитися за рахунок того, що завдасть компанії великої шкоди. Мовляв, «От ви думали, що я ні на що не зда тен ось вам, масте!»

Проте тут не йдеться про промислове шпигунство. Це явище, котре в Радянському Союзі називалося терміном «ініціативне шпигунство». Це кати радянські громадяни самостійно шукали контактів зі співробітниками іноземних спецслужб для передачі певної інформації. Ними займалася кон тррозвідка другого головного управління КДБ СРСР. Проте служба безпеки компанії неодмінно має звертати увагу на таких людей. Особливо, якщо вони мають доступ до закритої комерційної інформації.

Тут треба пам'ятати про елементарні правила. Одним з успіхів радянської розвідки колись став доступ до найсекретнішої інформації в офісі прем'єр-міністра Індії. Насправді за дуже смішні гроші наші колеги завербували дрібного клерка, який всього-навсього регулярно приносив їм використані копії з друкарських машинок секретарок. Його посада не передбачала доступу до секретної інформації, але був доступ до сміття. Як результат, у Москві знали про все, що друкувалося в офісі прем'єр-міністра.

Нині, певна річ, копірок немає. Однак є чернетки у смітниках. Питання у тому, чия рука писала ці чернетки. Особливо, якщо йдеться про президента компанії чи його заступників. Колись у Вашингтоні і в Москві були певні групи спеціалістів, які ретельно сортували сміття американського чи радянського посольства.

Виявлення злочинця на етапі шпигунства – як з ним бути? Чи варто доводити справу до суду (репутаційні втрати, розголошення тієї ж секретної інформації у суді)?

У цій ситуації є щонайменше декілька сценаріїв розвитку подій. Один з них може передбачати, приміром, дезінформацію конкурентів із використанням цієї людини

«насліпо». Це може тривати певний період часу, але в момент ключових операцій, скажімо, напередодні великого тендеру, у Вас буде можливість зіграти в цю гру. Всі інші варіанти залишаються на розгляд керівництва. Я не зустрічався із ситуаціями, коли компанії подавали до суду, хоч, можливо, вони і є. Якщо б мене запитали, що робив би я, то навіть не будучи громадянином СШЛ, я б зіслався на 5 поправку<sup>1</sup> до Конституції.

Як захищатися і не заробиш репутацію «параноїка»?

Я вважаю, що тут основним фактором має бути принцип розумної доцільності і оперативної необхідності. Людина повинна мати доступ виключно до тої інформації, яка потрібна їй по роботі. Якщо хтось продас покриття для підлоги, то йому не обов'язково знати закупівельні ціни на лак і фарбу. Розумна доцільність це ті заходи, котрі служба безпеки вважає необхідними для захисту інтересів своєї компанії. Це визначається рівнем компанії і родом її занять. Тут обов'язково мусить бути індивідуальний підхід. Коли мене запитують, скільки вартує пультова охорона, я ніколи не відповідаю, допоки не вивчу об'єкт. Це закон! Тут же йдеться про економічну безпеку компанії. Давати рекомендації, не вивчивши потенційного клієнта, — велика помилка.

Відкати. Це взагалі бич України. Як можна цьому протидіяти?

Тут, мабуть, справа не лише в маленьких зарплатах. У Північній Америці сикхів беруть на роботу в контролюючі органи, оскільки не існує зареєстрованих випадків хабарництва серед цих людей. Це релігія, культура, історія, загальом все, що формує менталітет нації. Рівень корупції у Канаді значно нижчий, аніж у США. Хоч вони сусіди і рівень життя приблизно однаковий. Тому все це визначається не лише економічним фактором. Для боротьби з цим злом потрібен комплексний підхід.



Мені доводилося зустрічатися зі скаргами клієнтів, коли вартість автівки купленої менеджером із продажів дорівнювала його трирічному заробітку. Можливо, рівень його оплати і рівень його повноважень були визначені не правильно. Можливо, неправильно була сформована політика продажів — такий рівень знижок був йому дозволений, за рахунок чого він і збагачувався. Це вже недопрацювання керівництва, вони мають краще розуміти конкурентоспроможність своєї продукції.

А практика відкатів іноді має і несподівані наслідки. Пайчасніше перші особи компанії відкати не носять і не виключено, що менеджер, який каже, що щось потрібно вирішити через відкат, частину відкачу або хабаря просто залишає у себе в кишені.

Скажу відверто, мені доводилося зустрічатися з людьми, які ніколи-ніколи, за жодних обставин не брали хабарів. Є особлива категорія партнерів, які відкатів не беруть пікши, — це власники бізнесу, котрі самі займаються управлінням.

Це система контролю закупівель у сукупності з високим рівнем матеріального стимулювання служби безпеки. Той хто економить на безпеці, потім розплачується за її відсутність.

Ми вже говорили про підбір персоналу. Так-от це і є найсерйозніше питання — підбір працівників служби безпеки і система субординації». Начальник служби безпеки є одним із найбільш високооплачуваних співробітників компанії і при ньому не підпорядковується нікому, окрім першої особи в компанії. У тих випадках, коли керівник

компанії і її власник це дві різні людини, го підпорядковуватися начальник служби безпеки має виключно власнику бізнесу. Це має глибоке переконавання.

А чи не буде у такий спосіб порушено принцип єдиноначальства?

Керівник СБ не підписує контракти, але він їх аналізує. У власника є інформація. Начальник особливого відділу військової частини не був офіцером Міністерства оборони. Це була військова контррозвідка — третє головне управління КДБ СРСР. Я не є прихильником радянської системи, але, коли мова йде про спецслужби СРСР, то треба визнати, що це була одна із найефективніших служб.

Звільнення співробітника, який мав доступ до секретної інформації, — як уберегтися від «шкідництва». «зливу» інформації з його боку?

Мені знову спала на думку 5 поправка. Це, звичайно, жарт. В кожному випадку треба вирішувати індивідуально, виходячи з психологічного портрету працівника, якого звільняють (чи він звільняється). В будь-якому випадку все має бути законно.

Ступінь вигоди і ризику від прийому працівника, який прийшов до вас з базами і інформацією від конкурента? Де гарантія, що він завтра не продасть вашу базу? З іншого боку, потрібно розуміти мотивацію, чому він пішов. Далеко не завжди у співробітника, що звільняється, є корисний мотив. Можливо, неправим був якраз роботодавець і це не значить, що та ж історія повториться з вами. Дружина дізналася, що чоловік закрутив роман із секретаркою і зруйнувала бізнес. Людині обіцяли — і не заплатили... Не йдеться про те, що каже сам працівник, за вдання спеціаліста — виявити. Гроші, сграх, любов, заздрість, влада — це основні мотиви людської поведінки. Спробуйте знайти.

І

Розмовляла Наталка Грицак