
Менеджмент безопасности II том
Кировоградский институт
имени Святого Николая
МАУП
В.Е.Карпов.
П.Ф.Закревский.
Менеджмент
безопасности
(теория и практика)
II том

Межрегиональная Академия Управления Персоналом

Кировоградский институт им. Святого Николая

Менеджмент безопасности

(теория и практика)

2 том

Кировоград
2007

ББК 88.59
УДК 159.98
К 26

Кировоградский институт им. Святого Николая МАУП.

Рецензент: **Н.А.Свирень**, кандидат технических наук, профессор, академик.

Менеджмент безопасности. (теория и практика)
2 том.В.Е.Карпов. П.Ф.Закревский. – Кировоград:
Кировоградский институт им. Святого Николая, 2007. – 340 с.

Научно-популярное издание. (В 2-х томах.) Рекомендовано к изданию Кировоградским институтом им. Святого Николая (КИиСН), Межрегиональной Академии управления персоналом (МАУП.) 340 стр. 2007. на укр..яз.

Под общей редакцией: В.Е.Карпова, доктора философии по психологии, член-корреспондента Международной академии проблем Человека в авиации и космонавтике, старшего преподавателя КИиСН МАУП.

Авторы издательства «Менеджмент безопасности» не претендуют на абсолютность изложенного материала, они подчеркивают, что в своей роботе использовали наработки известных ученных, специалистов, и при этом высказывают глубокую благодарность авторам других издательств, специализированных учебников и методических пособий.

Книга охватывает основные проблемы «Менеджмента безопасности» на современном этапе с учетом специфики организации безопасности государственных учреждений, предприятий различных форм собственности, банков, фирм и личной предпринимательской деятельности. Рассчитано на студентов, курсантов, слушателей переподготовки и повышения квалификации кадров, руководителей подразделений и служб безопасности, массового читателя.

ББК 88.59

В. Е. Карпов
П. Ф. Закревский

Зміст

ПЕРЕДМОВА

Підготовка державних службовців високого рангу, вимагає наступного поліпшення навчальних програм ВУЗів України. Наше суспільство на даному етапі розвитку характеризується цілим рядом реформ у політичній, правовій, економічній й іншій сферах життєвих інтересів громадян. Реалії сьогоднішнього дня висувають перед Вищою школою – більші проблеми підготовки якісно нових керівників з різних напрямків людської діяльності.

Дана книга націлена на підготовку студентів коледжів, вищих навчальних закладів, слухачів системи перепідготовки й підвищення кваліфікації кадрів, викладачів, фахівців і керівників підрозділів, служб, підприємств різних форм власності, а також масового читача. У книзі на основі широкого використання сучасних наукових подань, досвіду практичної роботи, розкриваються основні концепції й методи кадрового менеджменту безпеки, системи керування персоналом вітчизняних підприємств. Приводяться практичні, психологічні й соціологічні методики вивчення ефективності кадрової роботи й менеджменту безпеки на виробництві.

Знання отримані по ходу вивчення курсу (менеджмент безпеки), сформують у студентах, курсантах, слухачах, фахівцях і керівниках служб – аналітичні, практичні й науково сучасні навички, уміння, які будуть базуватися на правовій основі й широкому аспектному підході до рішення по-різному планових проблем з урахуванням людського фактора. Молоді фахівці й майбутні керівники середніх і вищих ланок, зможуть удосконалити свої знання, досягти вершин свого професіоналізму.

У першому томі книги “ Менеджмент безпеки ” знайшли основні методи аналізу й проектування систем керування, як правильно запровадити в життя ефективне керування на практиці, знання й розуміння завдань соціального розвитку підрозділів, умінням вирішувати щоденні проблеми розвитку колективу, мати необхідні юридичні знання, уміти застосовувати на практиці сучасні економічні методи керування персоналом.

Зацікавленому читачеві були представлені основні державно-правові функції теорії керування, їхня роль і місце в загальному керуванні суспільними процесами. Сформували уміння орієнтуватися в “Менеджменті безпеки” й ефективного використання в практичних цілях, також у Вас виробиться вміння високої правової й управлінської культури, пра-

восвідомості. Успіх роботи з людьми визначається знаннями менеджменту правових наук, психології, логіки, економіки, знаннями про людський фактор й т.д. Теорія державного керування, (інших форм керування)- охоплює широкий спектр проблем, від зв'язків держави із суспільством через механізм формування й реалізації керування до ефективності прийняття й впровадження управлінських рішень у життя.

У другому томі читач, що вже має мету й упевненість про правильність обраного шляху – знайде необхідні знання про менеджмент безпеки та практичну діяльність менеджера безпеки. Методах його роботи, навичках, планах, постановки завдань і перетворення їх у життя. В книзі буде поставлене питання: Менеджер безпеки, хто він, професіонал, керівник, бізнесмен, юрист, організатор – банкір, практик ? На перший погляд – це людина, що володіє необхідними вище перерахованими знаннями, які необхідні йому для роботи. Друге – це якість висококласного фахівця, що вміє не ординарно й оригінально мислити, добре розвинена інтуїція й інтелект, умінням працювати з людьми в різних напрямках.

Все це в першу чергу відноситься до державних підприємств й організаторів вищого класу, які приймають рішення й представляють престиж держави, захищають державні інтереси на міжнародному рівні, а також – інших керівників і спеціалістів підприємницької діяльності.

Наведемо приклад, у сучасній практиці керування США, (державні службовці приймаються на роботу на конкурсній основі і професійна служба – ділиться на 18 рангів):

- 1-8 найнижчий персонал – конторські працівники, техніки, стенографістки, кур'єри й т.д.
- 9-12 низький керівний склад – старші працівники в певній службі.
- 13-15 керівники середнього складу – менеджери по напрямках діяльності.
- 16-18 вище професійне керівництво. Все це спонукає зайняти ще вищий рівень управління.

Другий тім книги також розрахований на масового читача, менеджерів, керівників і бізнесменів підприємницької діяльності, з урахуванням характеру й рівня підготовки, психологічної установки й соціального стану. Автори й видавці книги прагнули дати максимально необхідні відомості для забезпеченні безпеки підприємства, банку, фірми й особисто підприємця. Варто врахувати, що в цьому процесі знайдуться небажані люди, які по тим або інших мотивах, будуть перешкоджати розвитку

підприємництва, не гидуючи ніякими засобами, часом ідуть на різні злочинні дії.

У сучасних умовах, у нашій країні проблема безпеки є дуже актуальною, тому що без її неможливо забезпечити безпеку бізнесу. Незважаючи на очевидність особливої значимості захисту підприємницької діяльності, проблема її забезпечення не стала пріоритетної для більшості бізнесменів України. Про це свідчить відсутність відповідних служб безпеки приблизно в половини комерційних фірм, низькі витрати банків і фірм на їхнє утримання, а також недостатня компетентність значної частини перших осіб у складних питаннях особистої безпеки й безпеки своїх структур, наявність у них кримінальної, "біловоротничкової криши", і противоправний характер діяльності певної частини недержавних підприємств.

Підприємець, не знайомий із цією проблемою, не може вважати себе повною мірою підготовленим для роботи в умовах ринкової економіки, коли законодавча база "кульгає", а корупція народжує боротьбу між суб'єктами ринкових відносин. Випускник будь-якого ВУЗа, де б він не почав працювати, скрізь і завжди буде зіштовхуватися із проблемами безпеки підприємницької діяльності.

Книга написана простою, доступною мовою, без зайвих міркувань, побудована на конкретних життєвих матеріалах, тому що автори в силу специфіки своєї роботи, впритул зіткнулися з даною проблемою, а, з огляду на, те, що для її викладення немає належної кількості практичних посібників по підприємницькій безпеці, автори на основі дослідження вітчизняного й закордонного досвіду по забезпеченню безпеки підприємницької діяльності, аналізу й узагальнення особистого досвіду роботи, підготували й написати книгу " Менеджмент безпеки".

Автори не претендують на абсолютність даної книги, вони підкреслюють, що в своїй роботі використовували напрацювання відомих вчених, провідних спеціалістів, при цьому висловлюють глибоку вдячність авторам інших видавництв, спеціалізованих підручників і методичних посібників : Р.М.Макарову – доктору педагогічних наук, доктору психологічних наук, професору, академіку; В.П.Петкову – доктору юридичних наук, професору, академіку; М.О.Свіреню – кандидату технічних наук, професору, академіку – людині з великою відданістю своїй праці та унікальними організаторськими здібностями. Особлива подяка Шмідту В. Ф. – дійсному членові Міжнародної академії

проблем Людини в авіації і космонавтиці, доктору філософії з інженерної психології, автору монографічного видання по інженерно-психологічному тестуванню. Іншим відомим вченим і викладачам ВУЗів, не зазначених в ступній частині книги.

Окрема подяка провідним спеціалістам СБУ та УМВС України в Кіровоградській області, ретельної уваги заслуговують наробітки колишніх працівників спеціальних підрозділів по боротьбі з економічною і організованою злочинністю та інших висококласних спеціалістів.

Автори, опираючись на думки спеціалістів, постаралися викласти матеріали, від сполучення теоретичного висвітлення проблеми, і загальних положень – до принципів, системи й організації забезпечення безпеки, та надали практичні рекомендації з поводження у звичайних й екстремальних ситуаціях, по організації роботи охоронних служб, забезпеченню безпеки кредитної політики й комерційних таємниць підприємств, банків і фірм, необхідним знанням по вивченню партнерів й емітентів, поверненню кредитів і багато чого іншого з напрямку безпеки підприємств.

Окремі розділи присвячені оперативній діяльності, добування комерційної інформації, інформаційно-аналітичній роботі, режиму й охороні, захисту електронно-обчислювальної техніки, каналів зв'язку й інші питання служби безпеки підприємства, банку, фірми, які необхідні для забезпечення безпеки підприємницької діяльності з урахуванням прогнозування можливих злочинів у бізнесі. Тому що війна розумів у бізнесі й банківській справі вже вступила у вирішальну фазу. Матеріали книги значною мірою задовольнять вимоги підприємців, фахівців, керівників різних рівнів і напрямків, і буде їм "настільною книгою", для того щоб убезпечити себе, свою діяльність, своє підприємство.

У книзі викладаються доступна інформація про стан злочинності в нашому суспільстві, дається наукова по суті й у той час вражаюча за формою картина різновидам організованої злочинності. Не багатослівно, але переконливо й ненав'язливо показується коротка історія її виникнення, препаруються зміст і структури організованої злочинності, розкриваються основні її елементи.

Окремі розділи книги – пропонують безліч методик по рятуванню від нападу в небажаному стані й виходу з нього. Можливо, на перший погляд читачеві здадуться деякі з них наївні, але всі рекомендації перевірені на практиці й тому дійсні. Тим більше, що вони мають значення, коли мова

йде про такі важливі обставини, що зустрічаються в житті, як викрадення і взяття заручників, вимагання грошей, викуп та великі матеріальні й грошові втрати, і багато іншого .

Окремої оцінки заслуговує технічний персонал по виданню та напрацюванню матеріалу: молодий та перспективний спеціаліст в області психології Кіровоградського ВДАІ при УМВС України в області – Пташкін О. П., а також провідні спеціалісти в галузі технічного забезпечення; Власенко В.П., Плаксієнко Л.Л. та Дуднікова Л.В., відповідальність яких дозволила провести кропітку роботу по викладенню книги « Менеджмент безпеки.»

Автори зазначають, що будуть вдячні читачам за зауваження і пропозиції, направлені на подальше вдосконалення даного видання.

Автори

Розділ 1.

Бізнес – розвідка

Програмна анотація

1.1. Основні завдання бізнес-розвідки у економічній сфері,

– розвідка служби безпеки підприємства,

– техніка бізнес-розвідки,

– інформаційна робота в бізнес-розвідці.

1.2. Вивчення конкурентів

– ділова розвідка для бізнесменів,

– загальний аналіз інформації про потенційних партнерів.

1.3.Підприємницьке шпигунство в системі інформаційних злочинів

– конфіденційна інформація та комерційна таємниця,

– незаконне збирання інформаційних відомостей.

1.1. Основні завдання бізнес-розвідки у економічній сфері

Якщо спробувати проаналізувати причини падіння результативності підприємництва в Україні, то більшість з них можна звести до одного – це невміння, а деколи і просто небажання, займатися обробкою і аналізом інформації, що є у розпорядженні бізнесмена, про ту, що оточує його, часто достатньо агресивною, середовищу.

На жаль, цей факт тільки починає привертати увагу більшості сьогоднішніх підприємців, і мало хто з них може визначити тип необхідної для його підприємства інформації, кваліфіковано організувати її пошук, уникнути ефекту дезинформації, уміло використовувати отриману інформацію при ухваленні рішення і для організації поточного контролю підприємницького проекту.

З іншого боку – останнім часом багато комерційних банків, стурбовані поверненням кредитних ресурсів, не тільки здійснюють ретельну перевірку передбачуваного позичальника, але і у разі потреби здійснюють інформаційну підтримку позичальника в цілях додаткових стабілізаційних заходів по забезпеченню безпеки повернення позикових засобів.

Реалії сьогоднішнього дня і тенденції подальшого розвитку українського бізнесу диктують необхідність осмислення і якоїсь формалізації підходів, що склалися, до рішення розвідувальних і контрозвідувальних завдань в економіці. Як показує і міжнародна практика, це питання повинне вирішуватися з двох сторін.

Бізнесмени повинні більше уваги приділяти створенню власних інформаційних ресурсів і їх захисту. Цьому повинні сприяти спеціальні освітні програми, семінари з обміну досвідом, дослід-ницька робота в даному напрямі академічних інститутів і технікумів.

Завдання розвідувальної і контррозвідувальної діяльності у сфері економіки полягає в попере-джуючому виявленні джерел зовнішніх і внутрішніх погроз безпеці підприємств, що максимально знижує невизначеність стратегічного ризику. Такого роду діяльність повинна забезпечувати керів-ництво господарюючого суб'єкта інформацією про дійсні наміри потенційних і дійсних партнерів, про сильні і слабкі сторони конкурентів, дозволяти робити вплив на позицію зацікавлених осіб в ході пе-

реговорного процесу, сигналізувати про можливе виникнення кризових ситуацій, дозволяти контролювати хід реалізації і дотримання партнерами досягнутих раніше домовленостей, виявляти несанкціоновані канали просочування конфіденційної інформації про фірму через обізнаність про нього партнерів, клієнтів і конкурентів.

Держава з свого боку повинна зробити крок назустріч вітчизняним виробникам і організувати максимально відкритий доступ до несекретної інформації, що є у нього. Повинна бути вироблена комплексна програма по використанню інформаційних ресурсів, що є у держави (можливо навіть на відшкодувальній основі). Адже втрати у разі провалу інвестицій значно перевищують витрати на отримання попередньої інформації.

Також необхідна і законодавча допомога держави у формуванні комерційних інформаційних структур. Адже рання діагностика кримінальних і шахрайських схем – це не тільки поповнення нашого багатостраждального бюджету за рахунок виплачених податкових зборів, але і якоюсь мірою спроба оздоровлення вітчизняного бізнесу, переклад його із стадії "розбирань в підворітті" хоч би в якусь подібність цивілізованих рішень.

Зараз не час ставити питання про принципову обгрунтованість і виправданість розвідувальної і контррозвідувальної діяльності в економіці. Ніяка стратегія, ніяка виробнича і комерційна політи-ка, а, отже, і капіталовкладення, науково-дослідні роботи, структурні зміни і т.д., не є відтепер можливими без поглибленого вивчення сил, рушійних миром: технології, економіки, політики і т.п. Зараз, більш ніж коли-небудь, стає ясно, що в конкурентній боротьбі, що розгорається, саме інформація забезпечить вирішальну перевагу.

В умовах загострення конкурентної боротьби і зростання злочинності роль і значення розвідки служби безпеки підприємства постійно підвищуватиметься.

Такий висновок витікає не тільки з досвіду країн з розвиненою ринковою економікою, але також з усвідомлення вітчизняними підприємцями практичної потреби отримання знань поперед-жуючого характеру про тенденції, факти, явища і т.п., що існують поза підприємством.

Інформацію такого роду здатна надавати (при належній організації її роботи) розвідка служби безпеки.

Підрозділ розвідки служби безпеки підприємства

Перед цим підрозділом зазвичай ставиться одна загальна мета: своєчасне виявлення і надання керівництву підприємства закритої інформації про реальні і потенційні зовнішні погрози його функціонуванню.

Звичайно, мета розвідки може бути сформульована і іншим чином, але у будь-якому випадку вона повинна відображати наступні моменти.

По-перше, своєчасність виявлення і представлення споживачеві (тобто керівництву підприємства) необхідної інформації (абсолютно очевидно, що відсутність або запізнювання відповідної інформації не дозволить прийняти міри по ліквідації або нейтралізації погроз діяльності підприємства).

По-друге, необхідно поставляти споживачеві не всяку, а якісну інформацію. Такою вона буде в тому випадку, якщо встановлені:

а) важливість (здатність внести внесок до діяльності підприємства);

б) точність (надійність джерела і самої інформації);

в) значущість (цінність і правильне розуміння інформації).

Нарешті, по-третє, сфера дій розвідки повинна знаходитися в зовнішньому середовищі функціонування підприємства.

Саме зовнішнє середовище функціонування підприємства є об'єктом розвідувальної діяльності служби безпеки. Вона включає 5 основних напрямків:

1. Постачальників (юридичні і фізичні особи, що забезпечують підприємство і його конкуре-нтів матеріальними ресурсами, необхідними для виробництва конкретних товарів або послуг).

2. Маркетингових посередників (фірми, що допомагають підприємству в просуванні, збуті і розповсюдженні його товарів серед клієнтури), що включають:

А.) – торгових посередників (ділові фірми, що допомагають компанії підшукувати клієнтів і/або безпосередньо продавати їм її товари);

Б.) – фірми по організації руху товару (склади, транспортні підприємства і т.д.);

В.) – агентства по наданню маркетингових послуг (фірми маркетингових досліджень, рекламні агентства, організації засобів реклами і консультаційні фірми по маркетингу);

Г.) – кредитно-фінансові установи (банки, кредитні компанії, страхові компанії і т.д.).

3. Клієнтуру (окремі особи, що набувають товарів і послуг для особистого споживання; організації, що набувають товарів і послуг для використання їх в процесі виробництва; організації, що набувають товарів і послуг для подальшого перепродажу їх з прибутком для себе; державні організації, що набувають товарів і послуг або для подальшого їх використання у сфері комунальних послуг, або для передачі цих товарів і послуг тим, хто їх потребує; зарубіжні споживачі, виробники, проміжні продавці і державні установи).

4. Конкурентів.

5. Контактні аудиторії (будь-яка група, яка виявляє реальну або потенційну цікавість до підприємства або робить вплив на його здатність досягати поставлених цілей), що включають:

А.) – фінансові круги:банки,інвестиційні компанії, брокерські фірми, фондові біржі, акціонери. Б.) – засоби масової інформації (газети, журнали, радіостанції, телецентри і т.д.);

В.) – державні установи, чия діяльність здатна негативно впливати на роботу підприємства;

Г.) – цивільні групи дій (організації споживачів, екологічні об'єднання, групи, що представляють національні меншини і т.д.);

Д.) – місцеві контактні аудиторії (організації самоврядування, злочинні угрупування, первинні осередки суспільних рухів і партій і т.д.).

Завдання для досягнення мети бізнес-розвідки

Досягнення мети, поставленої перед розвідкою, можливо при реалізації наступних завдань:

- виявлення правопорушень, що зачіпають економічні інтереси підприємства;
- своєчасне інформування про методи, способи і осіб, що мають намір (або що виконали це намір) завдати збитку підприємству і/або його персоналу;
- сприяння правоохоронним, судовим і контрольно-наглядовим органам в притяганні до відповідальності юридичних і фізичних осіб, дії яких зачіпають інтереси підприємства-засновника.

У свою чергу, виконанню цих завдань сприятиме реалізація наступних функцій:

- вивчення негативних і кримінальних аспектів тіньової економіки і ринку;
- визначення ступеня надійності ділових партнерів;
- надання керівництву підприємства необхідної інформації до і під час проведення ділових переговорів;
- виявлення підприємств, що займаються недобросовісною конкуренцією;
- збір відомостей про осіб, що не працюють на підприємстві і замишляють або зробили злочину проти його персоналу і/або майна;
- перевірка осіб, що уклали з підприємством комерційний контракт;
- встановлення фактів привласнення іншими фізичними або юридичними особами загубленого майна підприємства;
- перевірка кредитоспроможності ділових партнерів;
- виявлення і документування фактів порушень прав власників товарного знаку;
- збір відомостей по цивільних справах відносно юридичних осіб або громадян, що раніше не працювали на підприємстві;
- виявлення серед осіб, що не працюють на підприємстві, займаються економічним шпигунством проти підприємства-засновника.

Загальні ступені організаційної структури бізнес розвідки

Цілі, завдання, функції і ін. основні питання діяльності розвідки зазвичай відбиваються в положеннях про розвідувальні підрозділи.

Викладені нами вище за міркування про цілі, завдання і функції розвідувального підрозділу служби безпеці, якщо вони будуть прийняті, у вирішальному ступені визначають його оргструктуру.

Оргструктура розвідки включає два види підрозділів (відділень, груп, секторів, співробітників): добувні і інформаційні. Основне призначення добувних підрозділів полягає в добуванні всіма доступними і такими, що не суперечать законодавству засобами і методами відомостей, документів, предметів і інших матеріалів, які представляють або можуть представити розвідувальний інтерес. Тому у складі цих підрозділів повинні бути наступні відділення (групи, сектори, окремі співробітники):

- Сектор по роботі з інформаторами;
- Сектор по виявленню і збору відкритих і закритих публікацій; прихованого спостереження; технічного забезпечення операцій, що проводяться;
- Сектор – проведення розслідувань і документування поведінки об'єкту, що вивчається.

Значення цих підрозділів таке велике, що на їх фінансування доводиться, по деяких підрахунках, близько 80% витрат всієї розвідки. Добувні підрозділи повинні бути орієнтовані на те, що необхідні відомості можуть бути перехоплені у людей, які причетні до процесу збору, передачі, накопичення, зберігання, пошуку і переробки інформації і видачі її для використання. Зрозуміло, найбільш цінними для розвідки будуть відомості, готові для використання, проте нехтувати інформацією, отриманою на ранніх етапах процесу роботи з інформацією, недозволенно.

Основні завдання інформаційних підрозділів розвідки полягає в оцінці, класифікації, аналізі і наданні керівництву підприємства обробленої розвідувальної інформації. До складу цих підрозділів входять:

1.) – аналітичне відділення (група, сектор),

2.) – відділення стратегічного планування,

3.) – довідково-інформаційний фонд (ДІФ),

4.) – група експертів і консультантів.

Між всіма підрозділами розвідки повинне бути чітке розмежування по таких параметрах як завдання і форма представлення результатів роботи (див. табл.)

Параметри результатів роботи бізнес-розвідки

NN пп Найменування	Завдання підрозділу	Форма представлення результатів роботи
1.Відділення (група, сектор) прихованого спостереження	Фіксація вказаних в завданні фактів	Довідка, протокол спостереження
2.Відділення (група, сектор) проведення розслідувань	Збір необхідної інформації, документів і предметів	Аналітична довідка; документи (або їх копії), предмети (або їх моделі)
3.Відділення (група, сектор) по роботі з інформаторами	Залучення до співпраці інформаторів і отримання від них інформації	Справа (досьє); аналітичні огляди; довідки по кожному повідомленню інформатора регулярну інформацію
4.Відділення (група, сектор) по технічному забезпеченню проведення операцій	Установка і експлуатація технічних засобів, їх надання співробітникам інших груп	Акти; кино-, фотокадри, звукозапис і т.д.
5.Відділення (група, сектор) по виявленню і збору відкритих і закритих публікацій	Встановлення переліку необхідних друкарських видань, їх придбання і витягання з них потрібних відомостей	Огляди; копії найбільш важливих публікацій
6.Аналітичне відділення (група, сектор)	Обробка, класифікація і аналіз закритих і відкритих розвідувальних відомостей	Розвідувальні зведення; довідки-меморандуми
7.Відділення (група, сектор) стратегічного планування	Оцінка і ранжирування зовнішніх потенційних погроз безпеці підприємства і планування заходів щодо їх запобігання (нейтралізації)	Проекти програм запобігання (нейтралізації) зовнішнім погрозам безпеці підприємства
8.Довідково — інформаційний фонд (ДІФ)	Зберігання і видача співробітникам потрібної інформації	Довідки; оригінали друкарських публікацій, мікрофільми і т.п.
9.Відділення (група, сектор) експертів консультантів	Кваліфікована оцінка представлених матеріалів	Експертні висновки; акти експертиз; довідки

Загальноприйнятим вважається твердження про те, що потенціал розвідки безпосередньо залежить від наявності і якості відповідних сил і

засобів. Під силами розвідки розуміються детективи, співробітники допоміжних служб (канцелярія, бібліотека і т.д.).

Вимоги до особи розвідника високі: освіта вища (юридична і/або економічна), швидка кмітливість, чесність, об'єктивна самооцінка, хороші аналітичні здібності, пунктуальність, гнучкість, здатність чітко формулювати і висловлювати (у усній і письмовій формі) свої думки, винахідливість, товариськість, самодисципліна.

Технічні засоби бізнес-розвідки

Найважливіших засобів розвідувальної діяльності – розвідувальна техніка. До неї відносяться:

- засоби проникнення (відмички, піро-стрічка, різаки, спеціальні засоби);
- підслуховуючі пристрої (приємо – передаючі пристрої, мікрофони, електронні стетоскопи, магнітофони, системи прослуховування телефонів, факсів, телексів);
- системи прихованого відеоспостереження (мініатюрні камери, пристрої з об'єктивом «голкове вушко», ендоскопи, теле-, фотоапаратура стеження);
- системи комп'ютерного шпигунства (система перехоплення комп'ютерної інформації, комп'ютерний крекер).

Згідно іншої класифікації до технічних засобів відносяться:

- засоби спостереження і пошукової техніки (біноклі, зорові труби, прилади радіолокацій, прилади бачення в темноті, прилади ультрафіолетової і інфрачервоної техніки і т.д.);
- засоби фото- і кінозйомки, відеозаписи;
- звукозаписна апаратура;
- засоби зв'язку.

Спеціальні засоби бізнес –розвідки

Спецзасоби, хоча вони і дозволені для використання, але практично співробітниками розвідки не застосовуються. Технічні засоби можна застосовувати при дотриманні наступних трьох умов:

1) не порушувати кримінальних заборон;

2) забороняється порушувати основні права і свободи громадян, окрім окремих випадків, передбачених (або не заборонених) законодавством ;

3) недопущення шкоди здоров'ю і життю правопорушників.

До найважливіших засобів належать інформаційні системи, покликані надавати допомогу детективам в зборі, обробці і аналізі розвідувальної інформації. Серед матеріально-технічних засобів своєю специфікою виділяються службові приміщення. Існують загальноприйняті стандартні вимоги, яким повинні задовольняти службові приміщення розвідувальних підрозділів:

1. приміщення підрозділу повинне мати тільки одні вхідні двері (що охороняється цілодобово) і бути обладнано охоронний-пожежною сигналізацією;

2. ДІФ (довідково-інформаційний фонд) повинен знаходитися в ізольованому приміщенні, при цьому право входу співробітників повинне бути регламентоване;

3. розвідувальний підрозділ повинен розміщуватися вище за перший поверх (у ідеальному варіанті – поза приміщенням підприємства);

4. повинне бути виділене окреме приміщення для прийому відвідувачів, пошти і т.д.;

5. співробітники добувних і інформаційних служб повинні знаходитися в роздільних приміщеннях;

6. керівникові розвідки повинні бути надані окреме звуконепроникне приміщення і персональний сейф.

Загальні методи бізнес-розвідки

У розвідувальній діяльності застосовуються переважно наступні методи:

- ✸ приховане спостереження за людьми і стаціонарними об'єктами;
- ✸ зашифрований опит осіб, які можуть надати цінну інформацію;
- ✸ вивчення предметів і документів закритого характеру;
- ✸ конфіденційне наведення довідок;
- ✸ зашифрований зовнішній огляд будов, приміщень і інших об'єктів.

Зрозуміло, не забороняється вивчення відкритих джерел інформації (газет, журналів, бюлетенів і т.д.), голосний зовнішній огляд об'єктів. Проте використання цих методів в розвідці практикується тільки як додаткові і другорядні методи. Про небезпеку використання відкритих джерел недвозначно попереджав колишній керівник ЦРУ США А. Даллес: «Збирати відкриту інформацію легко, але не менш легкио і підсовувати в неї де-

зинформацію». У будь-якому випадку відкриті джерела інформації перевіряються ще раз розвідувальними методами.

Наприклад, аналізуючи транспортну документацію (укладання угод, договір залізничного перевезення і т.д.), можна отримати уявлення про кількісних, а іноді і цінових параметрах товарообігу фірми, що цікавить нас. Проте, щоб це уявлення перейшло в точні знання, необхідно отримати від інформаторів, освітлюючих діяльність цієї фірми, ряд інших відомостей.

Взаимодоповнюючі один одного зведення інформаторів і аналіз основних документів дозволять дати точну і об'єктивну оцінку що відбувається в цій фірмі. Без застосування негласних методів отримати таку оцінку практично неможливо. Цей приклад підтверджує правило, якому повинна слідувати будь-яка розвідка: інформація, отримана з використанням легальних можливостей, повинна обов'язково перевірятися ще раз за допомогою негласних інформаторів.

Існує певний взаємозв'язок між методами і джерелами розвідувальної інформації (під джерелами розвідувальної інформації розуміється тріада: людина – документ – виріб (процес), кожен з яких здатний в принципі дати необхідні відомості). Це можна відобразити таким чином (див. табл.).

Основні методи отримання розвідувальних відомостей (за джерелами інформації)

Людина	Документ	Виріб (процес)
1.Опит співробітників конкуруючої фірми.	1.Вивчення судових документів.	1.Фотографування моделей, експонатів і т.п. на виставках і конференціях.
2.Опит співробітників свого підприємства.	2.Збір і аналіз відомостей, що містяться в засобах масової інформації.	2.Кино-, фото- і відеоматеріали.
3.Замасковані опити «вивуджування» необхідної інформації на конференціях, семінарах, симпозіумах і т.п.	3.Вивчення фінансових документів конкурентів.	3.Комп'ютерні програми.

Людина	Документ	Виріб (процес)
4.Проведення «помилкових» переговорів з фахівцями конкуруючої фірми про передбачуваний переклад.	4.Збір і вивчення проспектів, брошур, що видаються конкурентами.	4.Аналіз відходів виробництва.
5.Наймання на роботу службовця конкуруючої фірми для отримання відомостей; складових комерційну таємницю.	5.Аналіз відомостей, що містяться у відомчих виданнях.	5.Покупка товару конкурента у третіх осіб.
6.«Помилкові» переговори з фірмою-конкурентом щодо придбання ліцензії.	6. Збір копій документів правоохоронних і контрольний — надзірательних органів (у викладі преси, довідки і т.д.)	
7.Створення помилкових підприємств, які широко пропонують роботу фахівцям з конкуруючих фірм.	7. Копіювання документів.	
8.Негласне ознайомлення.	8.Використання загублених документів.	
9.Підслуховування розмов, які відкрито (не таївшись) ведуть між собою співбесідники.	9.Використання звітів (копій) по перевірках на поліграфі («детекторі брехні»).	
10.Бесіда із співробітниками правоохоронних і контрольно-наглядаючих органів.		

Абсолютно очевидно, що приведені приклади не можуть бути вичерпними і дані вони тільки як ілюстрація можливого взаємозв'язку між методами і джерелами розвідувальної інформації. У зв'язку з цим з'являється необхідність в розробці методологічних підходів до використання вищезгаданих джерел розвідувальної інформації, на основі яких співробітники розвідки можуть планувати свою роботу по добуванню необхідних відомостей.

Перш ніж представити свої міркування із цього приводу, автори вважають за необхідне підкреслити, що аналіз можливостей цих джерел проведений роздільно тільки з методичних міркувань, а на практиці вони взаємодоповнюють один одного. Найбільш важливим джерелом розвідувальних відомостей в тріаді «чоловік – документ – виріб (процес)» є, безу-

мовно, людина. М. Вольф, колишній керівник розвідки ГДР, із цього приводу відзначив, що «робота з людиною-джерелом ніколи не може бути повністю замінена чим-небудь...». Певну офіційну інформацію в цьому аспекті може дати посадову особу, громадський діяч, партійний функціонер і т.д.

Отримання якої-небудь інформації можливе і у особи, здатної по різних мотивах (хвастощі, балакучість) випадково видати важливу інформацію. Проте по-справжньому цінну інформацію можна отримати тільки від привернутих до співпраці інформаторів. Інформаторів розвідувального підрозділу можна умовно розділити на декілька груп:

1. Співробітники свого підприємства, що контактують через своє службове положення із зовнішніми джерелами інформації.

2. Персонал інших підприємств, установ і організацій, що мають доступ до циркулюючої усередині них закритої службової інформації.

3. Обличчя вільних професій або що не працюють, мають контакти із співробітниками інших підприємств, громадських організацій, партій, суспільних рухів і з представниками неформальних структур.

4. Співробітники розвідувального підрозділу служби безпеки, що упровадилися за завданням свого керівництва в інші підприємства, неформальні групи і т.д.

Слід особливо підкреслити, що вищезгадані інформатори (окрім співробітників розвідки) не обов'язково повинні чітко усвідомлювати свою роль і свідомо співробітничати із співробітниками розвідувального підрозділу. «У розвідувальній роботі розмежування між корисними зв'язками, знайомствами і довірчими відносинами вельми умовно», – помічає із цього приводу колишній високопоставлений співробітник радянської розвідки Судоплатов П.А.

Цінним джерелом розвідувальної інформації є документ. Іноді неможливо роздобути оригінал якого-небудь документа, тому удаються до отримання його копії, а як її придбати, розвідник повинен знати. Щоб добути той або інший документ для зняття з нього копії, необхідно заздалегідь скласти документограму (графічне зображення руху, динаміки процесів документації, що протікають на підприємстві від створення документа до моменту здачі його в архів). Це дозволить виявити ті вузлові точки, в яких можливо в принципі «зняття» необхідної інформації.

Основні етапи впровадження нової розвідтехніки

Процес розробки, створення і впровадження нової техніки в промислове виробництво умовно можна розділити на **шість етапів**:

- проблемні науково-дослідні роботи (1 етап);
- прикладні науково-дослідні роботи (2 етап);
- дослідно-конструкторські роботи; виготовлення, випробування дослідного зразка, коректування креслень (3 етап);
- виготовлення, випробування промислового зразка і відробіток технічної документації (4 етап);
- освоєння промислового виготовлення нової техніки (5 етап);
- освоєння не промислового використання нової техніки (6 етап).

Знання особливостей всього процесу дозволяє співробітникам розвідки своєчасно виявляти відкриття (1 етап), винаходи (2-3 етапи) і ноу-хау (4-6 етапів), і сконцентрувати свій розвідувальний потенціал на необхідних напрямах. Особливо важливим для його співробітників є придбання промислового зразка (його макету). Кінцевий продукт розвідувальної діяльності – інформація і докази.

Інформаційна робота в бізнес-розвідці

Інформаційна робота в бізнес-розвідки – це процес, в результаті якого сирі факти перетворю-ються на закінчену продукцію розвідувальної діяльності. Вся зібрана розвідувальна інформація на підставі її кінцевого використання класифікується по наступних **категоріях**:

1) сигнальна (або застережлива);

2) тактична (тобто інформація, яка вимагає негайних дій;

3) стратегічна (тобто інформація, яка збирається впродовж відносного довгого часу і аналізується);

4) доказова (тобто дані у формі документів і предметів, що представляються в правоохоронні, судові і контрольно-наглядові органи).

Вся зібрана і оброблена інформація представляється керівництву підприємства у формі розвідувального огляду, довідки-меморандуму, повідомлення і т.д. Не дивлячись на різноманіт-ність цих документів, їх інформація повинна містити:

а) виклад фактичних даних;

б) джерела інформації (відносно інформаторів без їх розшифровки);

в) виводи;

г) пропозиції.

Надійність джерела і достовірність інформації оцінюється керівництвом розвідки за допомогою цифрових і буквених шифрів оцінюється по наступних параметрах:

Надійність джерела:	Достовірність відомостей:
А – абсолютно надійне джерело Б – зазвичай надійне джерело В – досить надійне джерело Г – не завжди надійне джерело Д – ненадійне джерело Е – надійність джерела не можна визначити	1. Достовірність відомостей підтверджується даними з інших джерел. 2. Відомості, ймовірно, правильні. 3. Відомості, можливо, правильні. 4. Сумнівні відомості. 5. Відомості неправдоподібні. 6. Достовірність відомостей не можна встановити.

Наприклад, А.3.- означає, що у абсолютно надійного джерела відомості, можливо, правильні.

Докази, критерії та показники бізнес-розвідки

Збирання доказів включає наступні елементи:

1) пошук і виявлення доказів;

2) фіксацію виявленого в Документах;

3) вилучення доказів

Документування розвідувальної інформації здійснюється по трьом основним напрямам:

- встановлення осіб, що можуть бути свідками у кримінальній або цивільній справі;
- виявлення предметів, що можуть бути джерелами доказів;
- пояснення, висновки експертів, письмові і речовинні докази; фіксація дій правопорушників.

Об'єктивну комплексну оцінку результатів роботи розвідки можуть дати **тільки керівники** підприємства-засновника.

Критеріями роботи розвідувального підрозділу можуть бути:

1) точність і об'єктивність відомостей про осіб, що вивчаються;

2) якісне документування протиправних дій юридичних і фізичних осіб, направлених проти інтересів підприємства-засновника;
3) своєчасне і об'єктивне інформування про зовнішні реальні потенційні погрози і їх носіїв.

Показниками, що розкривають ці критерії, можна назвати наступні:
1) кількість зведень, оглядів, довідок-меморандумів загального характеру;
2) кількість цивільних справ, виграних за допомогою детективів;
3) кількість успішно проведених за допомогою розвідки ділових переговорів;
4) кількість виявлених ненадійних ділових партнерів;
5) кількість виявлених недобросовісних конкурентів;
6) кількість виявлених некредитоспроможних ділових партнерів;
7) кількість перевірок осіб, що уклали з підприємством контракти і т.д.

1.2. Вивчення конкурентів

Збір інформації про конкурента є безперервним процесом із зворотним зв'язком. Цикл починається з визначення потреби у відомостях для фірми і організації ресурсів для збору необхідних відомостей. Після того, як інформація зібрана, її слід обробити і проаналізувати; в результаті отримують бажані конфіденційні дані, які потім розповсюджуються серед керівників і в тих підрозділах організації, які потребують таких даних. Безперервний зворотний зв'язок забезпечує модифікацію циклу, коли це необхідно, і вдосконалення загального процесу. У міру виникнення нових потреб служби збору розвідувальних даних збирають і поширюють нову інформацію.

Не має сенсу навіть намагатися вести промислову розвідку, не маючи закінченої систематизації. Безглуздо чекати від окремого фахівця або від групи осіб, щоб вони знали, а більш того, могли оцінити такий об'єм даних. Отже, всякі дії, зроблені без такої системи, здійснюються при неповному обхваті корисної інформації і приведуть до неправильних результатів аналізу і, як наслідок, до невірних управлінських рішень. Навіть суб'єктивна, особисто отримувана інформація вимагає систематизації. Вірогідність того, що випадкову обмовку запам'ятають і передадуть тим, хто ухвалює ключові рішення, набагато вище, якщо почувший знає про її

важливість і про систему, в якій її можуть оцінити, включити у відповідний контекст і використовувати як потенційну корисну інформацію. Систематизація збору відомостей про конкурентів означає на практиці, що будуть знайдені і проаналізовані відповіді на питання наступного характеру:

- Що потрібно знати?
- Де можна отримати дані?
- Хто збере дані?
- Як збиратимуть дані?
- Хто аналізуватиме і інтерпретуватиме дані?
- Як краще зберігати отриману інформацію, щоб ефективно використовувати її в майбутньому?
- Як поширювати отриману інформацію, щоб відповідні особи розглядали її своєчасно?
- Як оберегти систему від "витоків" і саботажу?

Розвідка повинна бути орієнтована на всі програми або цілі діяльності фірми і не може бути організована на разовій основі. Тому обгрунтовані відповіді на ці питання і результати аналізу необхідно накопичувати в комп'ютерних базах даних строго обмеженого доступу. Розповсюдження інформації, крім періодичних бюлетенів і відповідей на особливі запити, можна полегшити, якщо зібрати профілі інтересів споживачів інформації і ввести їх в комп'ютер. Тоді при введенні нових даних співвідношення їх з профілями автоматично може дати розвідувальну інформацію, яку людина при оцінці даних могла б упустити (функція оцінки). Цей прийом забезпечує подвійну перевірку і швидке розповсюдження важливої інформації серед відповідних споживачів.

Навіть якщо постійна формалізована система ділової розвідки вимагає автоматизації і застосування комп'ютерів, початкові відомості можуть і повинні бути високо персоніфіковані. Персоніфікований характер даних, що вводяться, обумовлює не тільки необхідність автоматизованих пристроїв для обробки даних, але і наявність потрібних людей в потрібних місцях.

Фахівці з маркетингу – тільки невелика частина людей, які можуть бути учасниками даної системи. У ній повинні брати участь всі компанії, що управляють, а також персонал, відповіда-льний за збір і обробку розвідувальних даних. В деяких випадках тільки вищі керівники повинні

мати доступ в конкуруючі організації, урядові установи і інші організації і отримувати там корисну інформацію.

Таким чином, певним резервом є підвищення індивідуальної кваліфікації осіб, що збирають інформацію, але основний упор повинен робитися на правильне розміщення працівників в системі, на роз'яснення ним їх обов'язків і забезпечення їх простими засобами доступу до інформаційної системи.

Ділова розвідка для бізнесменів, або як захиститися від збитків з вини неблагонадійного партнера

У діловому житті нашої країни такі явища, як недобросовісна конкуренція, шахрайство у сфері кредитно-фінансових відносин, криміналізація бізнесу, нерідко стають негативною складовою ділових зв'язків. Інколи складається враження, що уникнути цього можна лише залишаючись осторонь підприємницької діяльності.

Для успішної діяльності на ринку будь-якому підприємству необхідна повна і достовірна інформація про споживачів, партнерів, конкурентів, товарні ринки, інвестиційні можливості і багато іншого. Особливо важливою ділова інформація є для фірм, що планують випуск нових товарів чи вихід на нові ринки. Наприклад, якщо підприємець хоче започаткувати власну справу в певному регіоні, він має знати, принаймні, чи не буде його бізнес конкурувати з діяльністю фірм, близьких до посадовців регіону. Іншими словами, система моделює безпечний і вигідний бізнес.

Майже всі бізнесмени згодні з тим, що перед укладанням контракту варто оцінити фінансове становище і перевірити благонадійність потенційного ділового партнера чи великого клієнта. Однак, хоч як дивно, далеко не завжди підприємці намагаються підстрахуватися хоча б елементарним наведенням довідок про майбутнього партнера.

Тому на ринку багатьох держав в тому числі і в Україні, існує таке поняття ,(послуга) – ділова розвідка, або «конкурентна розвідка»,і, звісно, – інформаційні агентства, які надають клієнтам подібні послуги.

За способами отримання інформації, система є повною протилежністю «промисловому шпигунству», яке передбачає вивідування інформації забороненими способами з закритих від широкого доступу джерел.

За «конкурентною розвідкою» стоїть цілком легальний збір інформації про «колег» по бізнесу з використанням відкритих джерел (Інтернет, виставки, наукові конференції і публікації, довідники тощо).

Данні, що цікавлять замовника, аналітики черпають переважно з відкритих джерел. Крім того, організації, що спеціалізуються на наданні інформаційних послуг вже добрий десяток років, встигли сформувати власні бази даних (на основі різноманітних довідників, газетних і журнальних статей, інформації з інтернету, регулярних обов'язкових звітів компаній у відповідних ЗМІ про фінансові показники діяльності тощо). Багато хто з них на договірних умовах співпрацює з Держкомстатом, має доступ до баз даних МВС, СБУ, податкової інспекції.

В інформаційних бізнес-довідках, цілком з відкритих джерел, висвітлюють:

- Відомості про державну реєстрацію
- Правова форма і форма власності
- Статутний капітал і частки засновників
- Офіційні відомості про засновників і керівників
- Юридична і фактична адреса, телефони, факс
- Обслуговуючі банки, розрахункові і валютні рахунки
- Види діяльності
- Володіння власністю
- Дочірні, материнські і корпоративно пов'язані компанії
- Фінансові показники (зокрема за минулі періоди)
- Обсяги експорту/імпорту
- Участь у арбітражних процесах в якості відповідача
- Ділова репутація підприємства і його керівників
- Відомості про участь керівників і засновників у керівництві і засновництві інших підприємств зі схожою назвою
- Висновок аналітиків про ступінь ризику при вступленні у ділові відносини

Загальний аналіз інформації про потенційних партнерів

Навіть професійна діагностика контрагента не завжди дає змогу визначити його комерційну порядність. Систематизований аналіз інформації про потенційних партнерів компанії багато в чому нагадує боротьбу з комп'ютерними вірусами — з удосконаленням методів діагностики контрагентів виникають дедалі нові схеми в аферистів. Вони давно навчилися створювати видимість благонадійності не лише на словах, а й на па-

пері. Один зі способів — купівля підприємства з хорошою кредитною історією або навіть фальсифікація тривалих партнерських відносин.

Наприклад, не так давно жертвою однією з таких схем став великий український банк, який видав великий кредит одній російській компанії. Коли настав термін погашення, з'ясувалося, що позичальник заборгував цілому ряду фінустанов, а його кредитна історія, яка здавалася аналітикам бездоганною, – виявилася фальшивою. З'ясували, що формувалася ця історія за специфічною методикою: перш ніж обдурити кредиторів, засновники компанії кілька років кредитувалися у дружнього російського банку, справно виконуючи взяті на себе зобов'язання.

Наступне ноу-хау — робота за частковою передоплатою з безстроковою відстрочкою платежу. Суть схеми проста. Несумлінний контрагент створює собі імідж респектабельної компанії, орендує солідний офіс у центрі міста, зачаровує партнерів, закуповує товар за частковою передоплатою і..., після третьої-четвертої закупівлі свідомо перепродує товар фіктивній фірмі. Часто з такого виду контрагентів «нічого взяти». Ні, судитися з ними, звісно, можна й треба. От лише власне майно у цих відповідачів зазвичай відсутнє, а суми на розрахункових рахунках наближені до нуля.

Ще складніше протистояти шахрайству з боку добросовісних партнерів, а точніше — з боку найманих працівників контрагентів, з яким склалися давні й продуктивні відносини. Зокрема, ніщо не заважає найманому менеджеру, який знає час передбачуваного відвантаження товару, зловжити службовим положенням і відправити за продукцією водія з липовою довіреністю. Обчислити навідника практично неможливо — не лише з допомогою заходів діагностики контрагента, а й під час слідства. Загалом, в цьому житті, на кожного фінансового штірліца знайдеться свій антиштірліц.

1.3. Підприємницьке шпигунство в системі інформаційних злочинів

В умовах науково-технічного прогресу інформація стає об'єктом специфічних суспільних відносин, що виникають з приводу її створення, накопичення, зберігання, обробки та використання, набуває товарного вигляду. Формування, обробка та використання інформаційних ресурсів здійснюється в процесі інформатизації різних галузей людської діяльності, шляхом застосування сучасних інформаційних технологій. Однак розширення застосування таких технологій призводить не лише до позитивних наслідків – реалії сьогодення зумовлюють поширення правопорушень у сфері інформації, зокрема, інформаційних злочинів.

Характерною ознакою підприємницького шпигунства є **наявність предмета злочину** (елемент об'єкта злочину, впливаючи на який, злочинне посягання завдає шкоди суспільним відносинам). В якості предмета злочину традиційно називають певні предмети зовнішнього світу, однак щодо предмета підприємницького шпигунства існують певні особливості, оскільки таким предметом слід визнавати інформацію. Інформація ж не може повною мірою вважатися "предметом зовнішнього світу" через свої нематеріальні властивості.

Правильне визначення предмета злочину є необхідною умовою пізнання суті підприємницького шпигунства. Поняття інформації в загальному вигляді ст.1 Закону України "Про інформацію": "**Інформація** – документована або публічно оголошена, відомості про події та явища, що відбуваються в суспільстві, державі та навколишнього природного середовища".

Згідно ч.3 ст.34 Конституції України, реалізація прав на здійснення інформаційних процесів може бути обмежена законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, захисту репутації або прав інших людей, запобігання розголошення інформації, одержаної конфіденційно, або для підтримання авторитету й неупередженості правосуддя.

Це зумовлює поділ інформації за режимом доступу на відкриту та інформацію з обмеженим доступом (ст.28 Закону України "Про інформацію"). Відповідно – ст.30 Закону "Про інформацію", інформація за об-

меженим доступом поділяється на конфіденційну та таємну. З приводу складу злочину, що розглядається (підприємницького шпигунства), інтерес становитиме власне конфіденційна інформація.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні, або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов. Громадяни, юридичні особи, які володіють інформацією ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, банківського, комерційного та іншого інтересу, та не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність до категорії конфіденційної, та встановлюють для неї систему (способу) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено ВР України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої є загрозою життю і здоров'ю людей.

Таким чином, власник інформації як в підприємницькій, так і в інших сферах, є незалежним в питанні визначення режиму доступу до інформації, крім випадків, передбачених законом, перелік яких має бути вичерпним. До конфіденційної інформації, таким чином, може бути віднесений досить широкий спектр питань в різних сферах життєдіяльності суб'єктів правовідносин. У тексті статті 1486 законодавець безпосередньо вказує, який саме різновид конфіденційної інформації покликана захищати зазначена стаття. Таким різновидом конфіденційної інформації є комерційна таємниця.

Законодавством України визначене поняття **Комерційної таємниці підприємства**. Це відомості, які не є державною таємницею, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, розголошення яких може завдати шкоди його інтересам. Склад і обсяг таких відомостей, порядок їх захисту, визначає керівник підприємства, або підприємець-громадянин.

В Україні не створено спеціального законодавства з приводу питань комерційної таємниці; існує лише підзаконний акт (окрім загального законодавства про інформацію) – Постанова КМ. України від 9.08.1993 р

“Про перелік відомостей, що не становлять комерційної таємниці” [11]. До таких відомостей належать:

– установчі документи і документи, що дають змогу здійснювати підприємницьку чи господарську діяльність (свідоцтва, ліцензії і т.д.), окремі її види;

– інформація по всіх встановлених формах державної звітності;

– дані, необхідні для перевірки відрахувань на сплату податків, інших обов’язкових платежів;

– відомості про кількість, склад співробітників, розмір їхньої зарплати в цілому, по професіях та посадах, наявність вільних робочих місць;

– інформація про порушення вимог екології, безпеки праці і розмірів заподіяних у зв’язку з цим збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємств у діяльності кооперативів, малих підприємств та інших організацій, які займаються підприємницькою діяльністю;

– відомості, які згідно з діючим законодавством підлягають опублікуванню.

Питання щодо змісту інформації, яка становить комерційну таємницю, є дискусійним. Це, зокрема, відноситься до кореляції понять комерційної таємниці та інтелектуальної власності [11, 23, 31-33, 35, 36]. Інформація може бути не лише об’єктом права власності, а й права інтелектуальної власності. Режим доступу до останньої може бути різним, зокрема, така інформа-ція може бути віднесена до категорії конфіденційної.

З точки зору цивільно-правової охорони виділяють **2 форми інтелектуальної власності: авторське право та право промислової власності**. При цьому до останньої належать право на винаходи, корисні моделі, промислові зразки, право на науково-технічну інформацію, а також право на секрети виробництва та інші інститути, що не охоплюються авторським правом [35], оскільки перелік об’єктів промислової власності згідно Паризької конвенції 1983 року не є вичерпним.

Прихильники цієї точки зору вважають, що комерційна та інші види таємниць, які охороня-ються спеціальними законодавчими актами, а також авторськими або патентним правом, секретом виробництва (ноу-хау) не визнаються. Таким чином, вони стверджують, що секрети виробництва однозначно не є предметом комерційної таємниці. Однак, сек-

рети виробництва – це інформація, що сприяє підвищенню ефективності виробництва та іншої доцільної діяльності, і яка не відома третім особам. У силу зазначених факторів вона має комерційну цінність. Власник такої інформації вживає необхідних заходів щодо збереження її конфіденційності (тобто, це конфіден-ційна інформація). Власник може вчиняти щодо своєї власності будь-які незаборонені законом дії.

Строк дії права на секрет виробництва, як правило, чітко не визначається, оскільки це інфор-мація має здатність вибувати з під контролю власника і ставати надбанням третіх осіб, і зумовлений строком дії умов збереження конфіденційності інформації. Таким чином, за змістом і виходячи з букви закону (ст.30 закону "Про підприємства в Україні" [6]) секрети виробництва можуть бути предметом комерційної таємниці. Російське законодавство (ГК РФ), наприклад, відносить його до службової та комерційної таємниць.

Інші дослідники вважають, що існують три загальновизнані в світі форми інтелектуальної власності: **авторське право, патентне право, та інститут комерційної таємниці**, тобто серед об'єктів промислової власності виділяють такі, що захищаються за допомогою патентного права, а також такі, захист яких здійснюється за режимом комерційної таємниці. Така концепція також має істотні вади, оскільки фактично включає інститут комерційної таємниці до промислової власності.

Однак слід зазначити, що, з одного боку, інформація, яка є об'єктом промислової власності, може й не становити комерційної таємниці, а з іншого – предметом комерційної таємниці може бути не лише та інформація, яка є об'єктом промислової власності або інтелектуальної власності взагалі. До речі, останнє положення і зумовлює назву складу злочину (ст.1486), предметом якого є відомості, що становлять комерційну таємницю – **підприємницьке шпигунство**, на відміну від традиційного терміну "промислове шпигунство" (рос. "промышленный шпионаж").

Комерційна таємниця, таким чином, – це особливий різновид конфіденційної інформації, що має дійсну або потенційну цінність, оскільки є невідомою третім особам за умови, що законода-вець не передбачає вільного доступу до неї, а власник чи уповноважена ним особа вживає заходів щодо охорони конфіденційності такої інформації. Склад відомостей, що становлять комерційну таємницю, визначається відповідним суб'єктом інформаційних відносин з урахуванням зазначених в законі обмежень. В такому вигляді є відомості (інформація), що ста-

новлять комерційну таємницю і виступають **предметом підприємницького шпигунства**.

Наступною обов'язковою об'єктивною ознакою підприємницького шпигунства є об'єктивна сторона, яка реалізується шляхом здійснення активних дій.

Стаття 1486 КК України передбачає відповідальність за два самостійні склади злочинів:

1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю;

2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це завдало великої матеріальної шкоди суб'єкту підприємницької діяльності.

Під незаконним збиранням відомостей, що становлять комерційну таємницю, слід розуміти добування протиправним способом відомостей, які відповідно до законодавства України становлять комерційну таємницю (ст.16 закону України "Про захист від недобросовісної конкуренції" [9, 13]). Здійснення підприємницького шпигунства в формі незаконного збирання відомостей, що становлять комерційну таємницю, спрямоване на організацію витоку інформації.

Протиправні способи збирання інформації

Відповідно до чинного законодавства, для того, щоб визнати діяння "неправомірним збиранням комерційної таємниці", спосіб збирання відомостей обов'язково має бути протиправним. Поняттям "протиправного способу добування" має охоплюватись і неправомірне обернення відповідних відомостей у володіння, в тому числі за умов правомірного доступу. Таким чином, протиправність збирання є обов'язковою умовою визначення певного діяння як злочинного.

Однак власне щодо злочину, передбаченого ст.1486 КК, закон не передбачає якогось певного способу вчинення злочину як обов'язкову ознаку об'єктивної сторони (тут йдеться вже не про "спосіб збирання", а про "спосіб незаконного збирання"), або як кваліфікуючу ознаку.

Способи вчинення незаконного збирання можуть бути різними, зокрема: вилучення, в тому числі викрадення, матеріальних носіїв інформації, яка становить комерційну таємницю (докуме-нтів, що містять відповідні відомості, або предметів матеріального світу, певні ознаки яких можуть бути досліджені з метою встановлення необхідної інформації [19]), незаконне дослідження носіїв опосередкованої інформації

(технічних демаскуючих ознак, що містяться у власних або відображених фізичних полях об'єктів, які захищаються, а також у їхніх слідах у навколишньому середовищі) [19, 24], незаконне ознайомлення з такими документами або предметами в будь-який спосіб, порушення таємниці повідомлень, організація витоку мовної інформації, одержання відомостей від осіб, які ними володіють за плату (в цьому випадку йдеться про осіб, які не мають права розпоряджатися відповідною інформацією) чи шляхом застосування погроз або насильства.

Зазначені дії (як і інші злочинні дії в інформаційній сфері) також можуть бути вчинені фізичним (безпосередні дії людини, що завдають шкоди інтересам, які охороняються законом, та правам суб'єктів інформаційних правовідносин, що спрямовані на організацію витоку інформації), чи технічним (організація витоку інформації технічними каналами) способами. Під каналами витоку інформації слід розуміти джерела інформації, середовища розповсюдження сигналів та апаратуру зйому інформації.

Фізичний спосіб скоєння в більшості випадків спрямований не на інформацію безпосередньо, а на її матеріальні носії (викрадення), в той час як злочини, що вчинені технічним способом, найчастіше не зачіпають цілісність та приналежність матеріальних носіїв. У сучасних умовах широке розповсюдження набуває технічний спосіб незаконного збирання інформації шляхом використання інформаційних мереж як глобальних (напр., Internet [14]), так і локальних. В якості прикладу таких злочинів можна навести викрадення баз даних з інформацією про клієнтів шляхом підключення до банківських інформаційних мереж.

Досить різноманітними є також засоби вчинення злочину технічними каналами. Для досягнення мети підприємницького шпигунства шляхом зйому інформації за допомогою технічних засобів застосовуються: акустичні засоби (спрямовані або вмонтовані мікрофони, вібродатчики), лазерні засоби зйому мовної інформації, засоби зйому інформації з дротів та комунікацій, засоби перехоплення побічних випромінювань, закладні пристрої, комп'ютерна техніка, в тому числі її інформативні частини. Засоби вчинення підприємницького шпигунства в формі незаконного збирання відомостей, що становлять комерційну таємницю, так само, як і інші ознаки об'єктивної сторони підприємницького шпигунства (місце, час та обставини вчинення), не мають значення для кваліфікації злочину, але можуть бути враховані судом під час призначення покарання винній особі.

Злочин у формі незаконного збирання з метою використання інформації, що становить комер-ційну таємницю, слід вважати закінченим з моменту вчинення дій спрямованих на незаконне збирання відомостей, що містять комерційну таємницю, незалежно від їх подальшого використання та настання шкідливих наслідків. Це значить, що склад підприємницького шпигунства в зазна-ченій формі є формальним.

Незаконне використання відомостей

Наступною формою об'єктивної сторони підприємницького шпигунства є незаконне використання відомостей, що становлять комерційну таємницю. Під незаконнім використанням відомостей, що становлять комерційну таємницю, слід розуміти впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять комерційну таємницю [9]. Таке поняття незаконного використання, яке міститься в Законі "Про захист від недобросовісної конкуренції", не може вважатися досконалим, оскільки, зазначаючи про використання "неправомірно здобутих відомостей", не враховуються випадки такого протиправного використання, коли інформація власне отримується правомірно (слід відрізняти від неправомірного збирання за умов правомірного доступу, про яке йшлося вище з приводу попередньої форми об'єктивної сторони).

Таким чином інформація, що містить комерційну таємницю, може бути надана суб'єктові на законній підставі для досягнення певної мети. В такому разі використання зазначеної інформації з іншими цілями означатиме порушення комерційної таємниці, тобто буде неправомірним. Крім того, неможливо не вважати використанням передачу або продаж інформації зацікавленим особам, тобто ті випадки, коли суб'єкт підприємницького шпигунства власноруч не здійснює впроваджен-ня у виробництво або врахування під час планування чи здійснення підприємницької діяльності відомостей, що становлять відповідно до законодавства України комерційну таємницю (це, взагалі, і відбувається найчастіше).

Якщо не вважати платну чи безоплатну передачу здобутої інформації, її використанням (передачу неправомірно здобутої інформації), це також позбавить сенсу обов'язкову ознаку суб'єктивної сторони незаконного збирання відомостей, що становлять комерційну таємницю, а саме – мету використання, оскільки, як вже зазначалося, найчастіше інформація незаконно збирається особою не для власних потреб, а для передачі

зацікавленим особам, і така передача буде кінцевою метою злочину. Таким чином, якщо не вважати платну чи безоплатну передачу інформації використанням, незаконне збирання інформації з метою передачі, а не з метою використання для власних потреб, таке незаконне збирання не буде розглядатися як злочинне.

Крім того, злочином не буде, в такому разі, і передача зацікавленим особам інформації суб'єктами користування такою інформацією без згоди уповноваженої на це особи (що, власне, є використанням інформації не для тієї мети, для досягнення якої інформація надавалась на законних підставах, про що йшлося вище).

Обов'язковою ознакою об'єктивної сторони незаконного використання відомостей, що містять комерційну таємницю, є наслідки у вигляді заподіяння великої матеріальної шкоди суб'єкту підприємницької діяльності, тобто шкоди, яка в 50 та більше разів перевищує встановлений законом неоподаткований мінімум доходів громадян на місяць. При визначенні розміру заподіяної шкоди слід враховувати прямі матеріальні збитки, витрати на відвернення шкідливих наслідків використання відомостей іншими суб'єктами підприємницької діяльності, затрати на перепрофі-лювання напрямків діяльності, збитки від зниження попиту або цін на товари та послуги.

Заподіяння внаслідок злочину моральної шкоди суб'єкту підприємницької діяльності (наприклад, підрив ділової репутації) на кваліфікацію не впливає, але має враховуватись при призначенні покарання судом. Склад злочину, таким чином, є в даному випадку матеріальним.

Суб'єктом підприємницького шпигунства як в формі незаконного збирання відомостей, які містять комерційну таємницю, так і в формі їх незаконного використання, може бути фізична осудна особа, яка досягла 16-річного віку. Таким чином, суб'єктом підприємницького шпигунства є загальний суб'єкт. Разом з тим, не виключаються випадки скоєння підприємницького шпигунства спеціальним суб'єктом, наприклад, посадовою особою. В таких випадках, за наявності ознак посадового злочину, кваліфікацію слід проводити за сукупністю.

Суб'єктом незаконного використання відомостей, що містять комерційну таємницю, є особа, яка власне здійснює використання зазначених відомостей, незалежно від того, ким були зібрані використовувані відомості. Якщо збирання інформації було здійснене тією ж самою особою, яка здійснює незаконне використання такої інформації, необхідно

розмежовувати, суб'єктом яких саме дій (якої форми підприємницького шпигунства) є особа.

У випадках, коли йдеться про незаконне використання відомостей, ознайомлення з якими або одержання яких було здійснене на законних підставах (наприклад, особа, якій інформація, що становить комерційну таємницю, була надана для досягнення певної мети, використовує інформацію для інших цілей, не погоджених із суб'єктами розпорядження інформацією), винну особу слід вважати суб'єктом підприємницького шпигунства в формі незаконного використання відомостей, що містять комерційну таємницю, звісно, за умови, якщо таке використання завдало великої матеріальної шкоди суб'єкту підприємницької діяльності.

Якщо йдеться про випадки використання зазначеної інформації, яка була зібрана тією ж особою в незаконний спосіб (незаконність використання в цьому випадку зумовлена незаконністю збиран-ня інформації), особу слід визнавати суб'єктом підприємницького шпигунства в формі незакон-ного збирання з метою використання відомостей, що містять комерційну таємницю. Це зумовлено, так би мовити, більшою суворістю підходу законодавця до визнання таких дій злочинними: для визнання підприємницького шпигунства в формі незаконного збирання відомостей закінченим злочином не вимагається настання наслідків у вигляді заподіяння шкоди, так само, як і акту використання незаконно зібраних відомостей (за умови, що збирання здійснюється з метою використання). Таким чином, особа, яка використовує інформацію, яку попередньо зібрала незаконним шляхом, має нести відповідальність за самий факт незаконного збирання з метою використання відомостей, що містять комерційну таємницю, незалежно від настання протиправ-них наслідків та розміру заподіяної шкоди.

Встановлення суб'єктом якої саме форми підприємницького шпигунства є винна особа, незважаючи на те, що всі вони містяться в одній частині статті 1486 КК України, і за них передбачена однакова відповідальність (навіть, якщо визнати особу суб'єктом і збирання, і використання, її дії неможливо буде кваліфікувати за сукупністю), має важливе значення, якщо в діях особи містяться ознаки і збирання, і використання інформації. Це зумовлене тим, що для збирання та використання передбачених різних моментів закінчення злочину (в першому випадку – вчинення самої дії, в другому – настання передбачених законом наслідків), про що йшлося вище.

Проте можливі випадки, коли дії особи, яка незаконно зібрала, а потім використала відомості, що містять комерційну таємницю, будуть кваліфіковані як незаконне використання. За наявності передбачених законом наслідків у вигляді великої матеріальної шкоди, які необхідні для визнання незаконного використання закінченим злочином, винний не уникне покарання. Однак якщо така шкода заподіяна не буде, склад злочину в формі незаконного використання не відбудеться, і винний не буде покараний, незважаючи на те, що збирав відомості незаконним шляхом.

Таким чином, винна особа є суб'єктом:

- незаконного використання відомостей, якщо вони були отримані нею або іншою особою на законних підставах для іншої мети, або використання мало відбуватися за додержання певних умов, які особа порушила; такі відомості були незаконно здобуті іншою особою;
- незаконного збирання відомостей, якщо вони були в незаконний спосіб зібрані нею з метою використання, незалежно від того, чи відбувся акт використання; такі відомості були в незаконний спосіб зібрані нею та використані, незалежно від того, чи наявні наслідки використання у вигляді великої матеріальної шкоди.

Як вже зазначалося вище, незалежно від форми, в якій здійснюється підприємницьке шпигунство, суб'єкт цього злочину є загальним. На характеристику суб'єкта не впливає особливість об'єкта та предмета злочинних посягань, тобто цінність для здійснення підприємницької діяльності. Це означає, що суб'єктом підприємницького шпигунства не обов'язково має бути суб'єкт підприєм-ницької діяльності. Як правило, суб'єктами підприємницького шпигунства є особи, які (або за допомогою яких) реалізують зовнішні загрози інформаційній безпеці [26] суб'єктів підприєм-ницької діяльності (конкуренти, агенти конкурентів, особи, які не мають безпосереднього завдання конкурентів, злочинні елементи, партнери).

Такі особи можуть мати як корисливу, так і некорисливу зацікавленість в результатах своїх дій. Особливу категорію суб'єктів підприємницького шпигунства становлять співробітники фірми (різновид внутрішніх загроз) - вони можуть діяти як за завданням, так і без завдання конкурентів (останнє найбільш характерно для так званих "ображених співробітників").

Традиційно вважають, що співробітники фірми можуть бути суб'єктами лише розголошення комерційної таємниці - це положення до-

сить справедливе, однак не виключає і цілеспрямованого збирання ними з метою подальшої платної передачі певної інформації, якщо таке збирання є незаконним (наприклад, співробітник в силу службових обов'язків не має доступу до комерційної таємниці, однак незаконно отримує таку інформацію і продає її конкурентам), тобто здійснення ними підприємницького шпигунства. Це є характерним не лише для підприємницького шпигунства, а й для шпигунства взагалі.

В Україні суб'єктом злочину може бути лише фізична особа. Однак світовий досвід переконує в тому, що на підприємницькому шпигунстві спеціалізуються та заробляють чималі гроші навіть окремі юридичні особи, які використовують професійні, та здебільшого протиправні засоби отримання інформації [26]. Цікавим є, наприклад, той факт, що в США з 1986 року легально існує "Спільнота спеціалістів з добування відомостей про конкурентів" (SCIP), яка спеціалізується на відшуканні важкодоступної інформації, яка характеризує виробничі здатності та показники фірм, спосіб життя та схильності їхнього керівного складу (тобто, відомостей, які відносяться до комерційної таємниці відповідно до законодавства США), використовуючи як загальнодоступні, так і нелегальні засоби та способи [34]. В умовах впровадження сучасних інформаційних технологій в Україні і поширення підприємницького шпигунства та інших інформаційних злочинів дослідження цієї проблеми є дуже актуальним.

Висновок

В сучасну епоху масштаби економічного шпигунства різко зростають. Охота за чужими секретами дозволяє заощадити власні засоби на ведення прикладних і фундаментальних досліджень, бути в курсі справ конкурента, зосередити всю увагу на виробництві і маркетингу. Подальший розвиток науково-технічного процесу, збільшення потоку патентів і посилювання конкуренції як "війни всіх проти всіх" роблять викрадання чужих секретів особливо прибутковим і тому привабливим. Брами, ведучі, в пекло знаходяться напроти воріт, що відкриті в рай, - запевняє священна книга мусульман. Невідомо, як на небесах, але на землі конкуренція відкриває шлях і до достатку, і до задушення, бо конкуренція діалектична за своєю природою.

Конкуренція - це прогрес. Але вона ставить продуцентів в такі жорсткі умови, що вони вимушені поступати за принципом "переможців не судять", або "мета вища за засоби", що на практиці означає одне і те ж. Питання ставиться однозначно: або ти, або тебе пустять по світу. Третього

- не дано. Інакше кажучи, система диктує копити секрети і створювати розвідувальні структури, не жаліючи грошей на їх кадрове і технічне забезпечення.

Конкуренція і є боротьба в ім'я перемоги. Перемагає той, хто краще, якісніше і дешевше виробляє ту чи іншу продукцію, (послуги), що виражається в прибутку.

Це спонукає суперників невпинно шукати нові шляхи збільшення доходів. Це веде до прогресу. Переможець отримує завжди більше, ніж той, що програв. По суті, це універсальне правило.

У економічній конкуренції перемога не акт, а процес. Тому в конкурентній боротьбі вічних переможців не існує.

Розділ 2.

Інформаційна безпека підприємства

Програмна анотація

2.1. Інформаційно – аналітична робота

– основні завдання і структура інформаційно-аналітичного відділу безпеки,

– загальний перелік інформаційних елементів безпеки,

– принципові особливості інформаційно-аналітичної роботи.

2.2. Збір інформаційних даних про конкурентів

– аналіз і обробка інформації,

– система ділової розвідки проти конкурентів,

– безпека інформаційної системи підприємства.

2.3. Інформаційно-пошукова робота,

– інформація відкритого характеру,

– інформація закритого характеру,

– загальна обробка матеріалів засобів масової інформації, (ЗМІ),

2.4. Організація захисту інформації,

– основні вимоги до комплексної системи безпеки інформації,

– роль людського фактора в системі збереження державної та комерційної таємниці.

2.5. Організація захисту комерційної інформації,

– практичні дії на підприємстві.

2.1. Інформаційно-аналітична робота

Інформаційно - аналітична робота – це одна із основних внутрішньовиробничих функціональні складових безпеки підприємства.

Інформаційна складова полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства.

Належні служби підприємства виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової безпеки підприємства.

До таких належать:

- збирання всіх видів інформації, що має відношення до діяльності того чи іншого суб'єкта господарювання;
- аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів;
- прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів;
- оцінка рівня економічної безпеки за всіма складовими та в цілому, розробка рекомендацій для підвищення цього рівня на конкретному суб'єкті господарювання;
- інші види діяльності з розробки інформаційної складової економічної безпеки.

На підприємство постійно надходять потоки інформації, що розрізняються за джерелами їхнього формування. Заведено відокремлювати:

- відкриту офіційну інформацію;
- вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації;
- вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації.

Оперативна реалізація заходів з розробки та охорони інформаційної складової економічної безпеки здійснюється послідовним виконанням певного комплексу робіт, ми виділяємо 5 напрямків:

А. - Збирання різних видів необхідної інформації;

Б. - Обробка та систематизація одержаної інформації;

В. - Аналіз одержаної інформації;

Г. - Захист інформаційного середовища підприємства , що традиційно охоплює:

- заходи для захисту суб'єкта господарювання від промислового шпіонажу з боку конкурентів або інших юридичних і фізичних осіб;
- технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу заінтересованих юридичних і фізичних осіб до закритої інформації;
- збирання інформації про потенційних ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій з метою припинення таких спроб.

Д. - Зовнішня інформаційна діяльність.

Серед сучасних підприємців Заходу панує думка, що, використовуючи всього п'ять основних правил безпеки, можна добитися значних успіхів в бізнесі. До них відносять:

1.) розвідку;

2.) професіоналізм у встановленні контактів - мінімальні витрати часу і сил для пошуку інформації, необхідної для налагодження контакту;

3.) кваліфікацію менеджера - витрати часу тільки на потрібних людей;

4.) уміння долати перешкоди, пошук варіантів і обхідних шляхів для дозволу виникаючих проблем;

5.) уміння завершувати операцію, нехай навіть з негативним результатом - це все ж краще, ніж відсутність якого-небудь результату.

Отже, на перше місце ставлять розвідку. Чи випадково це? Тим самим, за допомогою якого розвідка робить вплив на проведення і розробку політики будь-якої фірми і забезпечення її безпеки, є інформація, що представляється своєчасно в усній або письмовій формі керівництву фірми. Виникає питання, яка ж потрібна керівництву фірми інформація ?. Хто і як повинен її готувати? Спробуємо відповісти на ці питання.

Так або інакше, сьогодні всі крупні і процвітаючі комерційні структури розвинених держав мають в своєму штаті підрозділи, які займаються інформаційною діяльністю. У одних фірмах - це інформаційно-аналітичний відділ, в інших - відділ маркетингу, на який керівництво фірми разом з іншими покладає і інформаційно-аналітичні завдання, в третіх - відділ ко-

мерційної розвідки. Часто все залежить від рівня розуміння керівництвом фірми ступеня важливості інформаційно-аналітичної роботи для безпеки всіх сторін діяльності будь-якої комерційної структури.

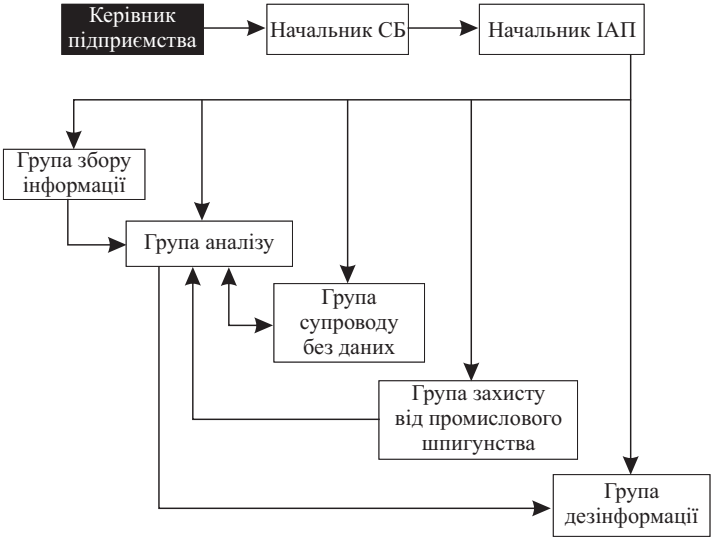
Основні завдання і структура інформаційно-аналітичного відділу служби безпеки підприємства

Основне завдання - збір інформації:

- про економічний стан фірми, регіону, своєї країни, країн, в яких є партнери і т.д.;,
- про політичну ситуацію в регіоні і країні; про морально-психологічний клімат в колективі;
- про конкурентів і методи конкуренції (добросовісною і недобросовісною);
- про кримінальні структури і можливі терористичні погрози;
- постановка завдань по перевірці потенційних партнерів, клієнтів, конкурентів;
- розробка програм протидії промисловому шпигунству, терористичним погрозам і іншим методам недобросовісної конкуренції;
- розробка програм дезинформації конкурентів:
- через засоби масової інформації;
- через інформаційно-телекомунікаційні канали;
- через постачальників, суміжників, партнерів, клієнтів;
- шляхом організації псевдопросочування конфіденційної інформації;
- розробка програм захисту конфіденційної інформації.

На малюнку №1 показаний зразок структури інформаційно-аналітичного підрозділу(ІАП).

Приблизна структура ІАП



Малюнок № 1

Завдання - обробка інформації:

Першою і найважливішою операцією є аналіз, який служить додатковим фільтром, що відкидає непотрібне і що є захистом від шуму без підстави. Ця операція полягає перш за все у визначенні важливості, точності і значущості інформації. Інформація є важливою, якщо вона зв'язана, тобто має зв'язок з елементами бази, і якщо вона здатна внести внесок до організації. Коли внесок значимий і безпосередній, інформація вимагає термінових дій.

Інформація, що не має значення, повинна бути виключена щоб уникнути втрати часу і енергії. Не завжди легко встановити, є інформація достовірною або помилковою, особливо якщо вона містить відомості про події, які ще не відбулися.

Допускається два критерії, по яких можна судити про точність інформації, надійність джерела і самої інформації. Головним критерієм правдоподібності є пошук підтвердження за іншими джерелами, якщо можливо – за незалежним.

Значущість інформації...

Інформація може бути важливою і точною і в той же час даремною, оскільки вона недостатня для розуміння і дії. Розвідка в бізнесі відноситься до даних про навколишнє середовище і конкурентів, аналізованим з метою використовувати їх в конкретній ситуації. Ні окрема особа, ні організація не можуть ефективно діяти в умовах конкуренції без глибокого розуміння цього середовища або не маючи в своєму розпорядженні новітньої інформації про те, що в ній відбувається.

Вид потрібної інформації залежить від виду компанії (фірми, її конкурентного середовища і багатьох інших характеристик самої фірми і її оточення. Сьогодні практично весь український бізнес в тому або іншому ступені має тіньові сторони: ухилення від податків, подвійна бухгалтерія, заниження і подальша підміна інвойсів, захована дійсного об'єму постачань, безготівкові операції через фірми-однодневки і ін. У такій ситуації фірма може стати заручником кримінальної структури, яка бере фірму під свій контроль (так званий "дах") і може використовувати її для відмивання власних нелегально отриманих коштів. Крім того, як "дах" можуть виступати і різні силові структури. Отже, необхідно постійно володіти інформацією про співвідношення сил і розділення сфер впливу в місті або регіоні, в яких знаходиться фірма, в ніші ринку, яку займає фірма.

Нарешті, практично всі фірми, окрім найдрібніших і фірм-однодневок, залежать від поточної і майбутньої розстановки політичних сил. Тому правильне прогнозування можливих змін у вищих ешелонах влади (починаючи з розділів міських і обласних адміністрацій) є основоположною умовою виживання фірми і стабільності її бізнесу.

Потреба в інформації варіюється залежно від здійснюваної або планованої діяльності. Компанія може мати довгострокові (стратегічні) плани, тактичні або короткострокові, плани і поточні операції; всі вони вимагають добре вивіреної інформації. У широкому друці іноді намагалися змалювати ділову розвідку про конкурентів як "шпигунство". Можливо, до деякої міри це дійсно так. Проте слід зазначити, що сьогодні переважна маса ділової інформації може бути отримана з відкритих джерел без порушення етичних норм. Список того, що хотіла б знати про конкурента ділова фірма, може бути нескінченним.

Зразковий перелік **потрібної інформації** може служити ілюстрацією корисності розвідки. Подробиці можуть мінятися від компанії до компанії, але є основні елементи, необхідні для більшості з них.

Інформація про ринок

1. Ціни, знижки, умови договорів, специфікації продукту.
2. Об'єм, історія, тенденція і прогноз для даного продукту.
3. Частка на ринку і тенденції її зміни.
4. Ринкова політика і плани.
5. Відносини із споживачами і репутація.
6. Чисельність і розміщення торгових агентів.
7. Канали, політика і методи збуту.
8. Бюджет і план рекламної кампанії.

Інформація про структуру виробництва

1. Оцінка якості і ефективності.
2. Номенклатура виробів.
3. Технологія і устаткування.
4. Рівень витрат.
5. Виробничі потужності.
6. Розміщення і розмір виробничих підрозділів і складів.
7. Спосіб упаковки.
8. Доставка.
9. Необхідність і можливості проведення НДР.

Інформація про внутрішню організацію і фінансове положення

1. Визначення списку осіб, що ухвалюють ключові рішення.
2. Філософія і психологічні установки осіб, що ухвалюють ключові рішення.
3. Фінансові умови і перспективи.
4. Програми інвестицій і кредитування.
5. Головні проблеми (можливості).
6. Програми НДР.

Подібний список може створювати враження, що розвідка проти конкурентів - просто набір даних. Насправді в цих даних повинна бути відображена поведінка конкурента як в короткостроковій, так і в довгостроковій перспективі.

Який же результат повинен бути продуктом діяльності інформаційно-аналітичного підрозділу фірми? До такого результату відносять виявлення глибинних зв'язків між розрізненими, на перший погляд,

подіями, засноване на їх оцінці і тлумаченні з урахуванням всіх зовнішніх (економічних, політичних, соціальних) і внутрішніх чинників впливу на діяльність фірми і визначення їх значення для вирішення конкретних завдань поточної політики фірми.

Такий підхід називається **системним**. Цим підкреслюється різниця між первинними матеріалами і остаточним продуктом діяльності інформаційно-аналітичного підрозділу.

Для ефективної роботи інформаційного підрозділу фірми керівництвом повинні бути чітко обкреслені його основні цілі. Ці цілі можуть полягати в наступному:

1). Забезпечити своєчасне надходження надійної і всесторонньої інформації про здібності і майбутні можливості кожного з основних конкурентів.

2). Визначити, яким чином дії основних конкурентів можуть зачіпати поточні інтереси фірми.

3). Постійно забезпечувати надійну і обширну інформацію про ті події в конкурентному оточенні і на ринку, які можуть мати значення для інтересів фірми.

4). Добиватися ефективності і виключати дублювання в зборі, аналізі і розповсюдженні інформації про конкурентів.

Принципові особливості інформаційно-аналітичної роботи

Працюючи над створенням системи інформаційного забезпечення фірми, важливо відзначити ряд ключових положень, ми виділяємо 8 таких положень:

1. Промислова розвідка діяльності конкурентів необхідна для забезпечення успіху в ринковій конкуренції.

2. В даний час ситуація на ринку міняється так різко, що формальних засобів спостереження за конкурентами недостатньо.

3. Методи “проб і помилок” в отриманні такої інформації зрештою неефективні. Для забезпечення функції розвідки потрібна тотальна система в повному розумінні цього слова.

4. Система промислової розвідки повинна бути дуже сильно орієнтована па конкретних осіб, навіть якщо її структура і організація постійні.

5. Така система повинна бути орієнтована на дії. Вона не повинна просто видавати звіти і накопичувати дані. Швидше вона повинна забезпечувати керівників такою інформацією, яка указувала

6. на необхідність дій і допомагала ухвалювати правильні управлінські рішення. 6. Конфіденційну інформацію можна отримати з різних джерел, багато з яких при поверхневому погляді можуть показатися малозначними або навіть даремними.

7. Система розвідки повинна передбачати завдання охорони власних секретів і контррозвідки. Ця рекомендація заснована на припущенні, що у конкурентів є аналогічні системи і що вони можуть удатися до незаконних або неетичних засобів для проникнення у ваші комерційні таємниці.

8. Система розвідки повинна бути ефективно організована без звернення до незаконних або неетичних методів збору даних.

2.2. Збір інформаційних даних про конкурентів

Дані для системи розвідки про конкурентів можуть поступати з різноманітних джерел, як державних, так і приватних. Люди, не знайомі з розвідкою, часто думають, що найкорисніша інформація здобуваються з секретних джерел. Вони вважають типовими для розвідки такі явища, як знамениті публікації про секретні операції ЦРУ.

Насправді велика частина розвідувальної діяльності зв'язана з використанням опублікованих відомостей. Це справедливо навіть для військових, прикладом чому може служити заява адмірала Захаріаса (заступника начальника військово-морської розвідки США під час другої світової війни) про те, що 95% інформації військово-морські служби США отримували з опубліко-ваних даних, 4% з напівофіційних даних, і лише 1% - з секретних джерел.

Отже, основна увага повинна концентруватися на організованому вивченні офіційно доступних джерел інформації. Значна частина основної інформації, використовуваної службами планування, може поступати звичайним порядком з численних публікацій про діловий світ в засобах масової інформації, промислових журналах, газетах, урядових виданнях,

навчальних посібниках або наукових працях, а також з постійного неформального потоку відомостей від торгових агентів.

Хоча багато відомостей можна отримати саме таким чином, наприклад, шляхом комп'ютеризованого пошуку через Інтернет і організованих пошуків в промислових бібліотеках, процес розвідки може бути дуже продуктивним і на самому нижчому рівні організації. Цінним складальником інформації може бути простій торговий агент, якому можна доручити відправитися на огляд конкуруючого підприємства і доповісти про свої спостереження відділу збуту. Клерк, що отримав завдання робити вирізки з газет тієї місцевості, де знаходиться конкурент, також виконує важливу розвідувальну функцію.

Як наголошувалося вище, накопичення даних приймає форму безперервного збору базових даних для тотальної розвідки або для ознайомлення з чинниками і силами, що діють в конкуруючих фірмах, і збору особливих відомостей для заповнення інформаційних пропусків в розвідувальних даних або для відповіді на спеціальний запит про конкурентів від певного менеджера - споживача інформації.

Фаза накопичення інформації включає формулювання напрямів діяльності, підготовку плану збору даних з вказівкою цілей і завдань і його передачу тим особам і установам, які відповідають за його практичне здійснення.

На першій стадії збору інформації ініціатива зазвичай належить розвідувальній службі, яка діє на підставі власного аналізу планових документів організації або ж на спеціальне прохання «споживача». Розвідувальна служба вибирає напрями своїй діяльності на підставі генеральної мети організації, а також спеціальних вказівок, що містяться в різних планах організації. Враховуються також вказівки менеджерів, штабного персоналу вищестоящих і підлеглих підрозділів організації. Ця служба винна, звичайно, бути обізнана про будь-які зміни в плануванні, особливо якщо міняються цілі і завдання організації. Відомості про нові напрями або можливі нові завдання організації мають кардинальне значення для збору адекватної і важливої ділової інформації.

Джерела потенційно важливої інформації і різноманітні способи її використання настільки численні, що наявність плану збору інформації абсолютно необхідна для успіху такої системи. План збору розвідувальних відомостей про конкурентів, співвідносить потреби в інформації з її

потенційними джерелами так, щоб уточнити і обмежити процес відбору такої інформації.

Нижче ми приводимо перелік джерел ділової інформації про конкурентів, а також опишемо можливий процес збору необхідних відомостей. Хоча джерела потенційних даних про конкурентів такі численні і різноманітні, що назвати їх всіх тут не можна, огляд цих джерел переконає читача в тому, що можна отримати необхідні для господарського керівництва дані про конкурентів і залишитися при цьому в рамках юридичних і етичних норм. Перелік джерел інформації, який можна доповнити залежно від потреб компанії, автори запропонувати наступний:

1. Торгові представники на місцях. Торгові агенти через часті контакти з клієнтами і іншими агентами є одним з кращих джерел інформації. Проте вони часто можуть бути носіями напівправди або невірної інформації, особливо в області цін. Їх відомості слід перевіряти ще раз через інші джерела.

2. Відділ постачання. Агенти по постачанню часто добре інформовані про те, що відбувається у даній галузі промисловості. Вони мають можливість часто відвідувати різні підприємства. Можна використовувати цю обставину і інструктувати агентів по постачанню, чим цікавитися.

3. Відділення досліджень і розробок. Науковці і конструктори стежать за технічними успіхами і відкриттями в своїх областях. Їх обертання в кругах фахівців і увага до технічних публікацій часто формує хороше уявлення про виробничу діяльність конкурентів.

4. Фінансовий відділ. Це джерело інформації теж може бути корисне; якщо конкурент одночасно і клієнт, фінансовий відділ знатиме, як він проводить оплати і яке його фінансове положення. Крім того, фінансовий відділ завжди може увійти до контакту з поважними особами у фінансових кругах, які мають докладні відомості про фінансовий стан конкурента.

5. Вищі керівники. Вищі керівники здійснюють часті контакти з своїми колегами в даній області промисловості. Ці контакти дають уявлення про те, що робить конкурент.

6. Ділові періодичні видання. Необхідно уважно вивчати ділову періодику у пошуках статей про діяльність конкурента.

- Урядові джерела.
- Професійні асоціації.
- Покупці. Постачальники.

- Збутові організації.
- Торгові асоціації.
- Місцева преса.
- Торгова преса.
- Біржові маклери.
- Проспекти.
- Збори акціонерів.
- Місцеві банки.

Аналіз і обробка інформації

Фаза аналізу включає статистичну комп'ютерну обробку, облік соціологічних, психологічних і соціальних аспектів діяльності об'єкту, що розробляється.

Зібрані дані не є інформацією до тих пір, поки вони не проаналізовані і інтерпретовані кваліфікованим експертом. У термінових випадках інформацію можна передавати особам, що ухвалюють рішення, без вивчення експертами, але, коли час дозволяє (тобто в більшості випадків), саме оброблені відомості особливо корисні тим, хто ухвалює рішення.

Якість аналізу і інтерпретації у великій мірі залежить від професійної приналежності аналітика. У господарській організації це означає, що найбільш відповідною особою для інтерпретації певної інформації є людина, що володіє відповідальністю у відповідній функціональній області (виробництво, маркетинг, фінанси, дослідження і розробки і т.п.). Визначення можливої стратегії конкурента в освоєнні нових ринків може здійснюватися декількома особами (організованими в робочу групу) – представниками декількох функціональних підрозділів організації. «Військова гра» для визначення стратегії конкурента може бути організована шляхом створення усередині організації «мікрокомпанії» для вивчення тих, що мають розвідувальну цінність даних і для подальших теоретизувань про можливу стратегію конкурента.

У будь-якому випадку необхідний централізований центр обробки інформації – у багатьох випадках спершу буває достатньо однієї людини. Наприклад, в одній компанії була призначена людина, яка почала з того, що розіслав «список розшуку», що містив питання про діяльність конкурентів по певних ключових програмах компанії. Щонеділі цей список оновлювався. Торгові агенти і інші співробітники, що отримали список, повинні були повідомляти у відділ розвідки все, що могло мати значення

про діяльність конкурентів. Таким простим способом вдалося зібрати багато відомостей про стратегію конкурентів в області технології і маркетингу, зокрема щодо важливого державного проекту, по якому компанія готувала свої пропозиції.

У іншому випадку розробка новітніх профілів конкурентів дозволила зробити вивід про новий крок конкурентів в області технології. Цей вивід був заснований на аналізі біографій осіб, у той час висунутих на відповідальні пости в організації конкурента. Обізнаність про рівень технічної підготовки і досвід декількох ключових співробітників компанії-конкурента дозволила зробити вивід про те, що її стратегія буде грунтуватися на досягненні технічної переваги. Компанія виробила стратегію ефективного суперництва з ним і зуміла добитися отримання декількох важливих контрактів.

Порядок перевірки надійності джерела і достовірності інформації , документування розвідувальної інформації , його напрямки та про комплексну оцінку результатів роботи розвідки ми детально розглянули в розділі Бізнес-розвідка.

Фаза ухвалення рішення включає порівняльну оцінку представлених виводів і рекомендацій з урахуванням тієї інформації, якою володіє тільки особа, що ухвалює рішення.

Розповсюдження інформації

Минулі оцінку розвідувальні відомості розповсюджуються потім серед відповідних осіб і відділів. Якщо по своєму характеру інформація відноситься до стратегічного планування, то її повинні отримувати особи, що становлять плани і що несуть відповідальність за ухвалення стратегічних рішень. «Делікатна» по характеру інформація може повідомлятися тільки окремим особам. У військових установах превалює принцип «знати тільки необхідне»: незалежно від положення співробітника в організації він повинен отримувати тільки ту розвідувальну інформацію, яка йому необхідна для виконання його обов'язків. Цей принцип застосовний в будь-якій організації.

Слід встановити правила розповсюдження інформації з тим, щоб забезпечити необхідну обережність, але і не відмовляти в інформації тим, хто її потребує.

Система ділової розвідки проти конкурента,
(з точки зору роботи ІАП)

Система ділової розвідки проти конкурента повинна підказувати керівникам, коли слід прийняти ті або інші заходи, і указувати, як це краще зробити. Якщо система просто безперервно видає томи звітів, то ініціатива у вживанні заходів повністю віддається керівникові; йому доводиться просівати масу даних для того, щоб оцінити надійність і корисність інформації. Щоб звільнити керівника від цієї роботи, система ділової розвідки повинна бути орієнтована на виняткові ситуації; це означає, що крім безперервного потоку важливої інформації, вона повинна забезпечувати сигнали про необхідність дій.

Останнє питання розробки системи ділової розвідки проти конкурентів стосується її підпорядкування: яке місце вона повинна зайняти в організаційній ієрархії і як вона повинна бути організована? Відповідь на це питання у великій мірі залежить від вимог, що пред'являються до системи, і у свою чергу визначає план діяльності.

Якщо вже діє ефективна система інформації про маркетинг, служба розвідки може увійти до складу цієї системи (більшість ділових фірм саме так розташовують цю службу в організаційній структурі). Проте таке досить низьке положення в ієрархії і прив'язка до однієї функціональної області (маркетинг) зв'язане з незручностями, оскільки може перешкоджати необхідній притоці інформації в інші функціональні підрозділи.

Оскільки в ідеалі розвідка проти конкурентів повинна відповідати на запити всіх функціональних підрозділів, досвід показав, що якнайкращі результати досягаються, якщо відповідна служба автономна і централізована в рамках певного напряму господарській діяльності. При великій диверсифікації виробництва служба розвідки може бути до деякої міри децентралізована.

Для успіху будь-якої програми необхідно, щоб була служба (можливо одна людина), що відповідає за координацію всієї розвідувальної функції, за збір, аналіз і розповсюдження інформації. Коли визначені права і обов'язки служби, можна почати роботу по збору інформації.

Виникає питання, як це слід робити, яка потрібна інформації? Це питання вимагає точності. Перерахуєте інформацію, істотну для планування. Визначите, що потрібно знати про конкурентів. Крім того, будьте реалістичні. Ніхто не може дізнатися всього, що він хотів би дізнатися.

Як слід отримувати інформацію? Оцініть всі потенційні джерела необхідної інформації.

Що забезпечує надійність інформації? Забезпечте участь в її пошуку інших підрозділів організації: відділи закупівель, фінансовий, технічний, виробничий і відділ контролю можуть не усвідомлювати, що вони здатні зробити внесок в оцінку конкуренції.

Як організувати інформацію? Існує багато способів організації інформації. Доведена виправданість ведення архівів на важливих конкурентів. Усередині такий архів підрозділяється на секції по основних категоріях інформації: маркетинг, продукт, виробничі потужності, організація і фінанси, сильні / слабкі сторони, можливі стратегії і ін.

Як аналізувати і серед кого поширювати розвідувальну інформацію? Якої політики і яких напрямів слід дотримуватися? Ми повинні вам сказати, що кожен керівник сам визначає політику і напрями використання розвідувальних відомостей про конкурента.

Безпека інформаційної системи підприємства

Створена в компанії система найважливішої інформації про конкурентів неминуче приведе до накопичення «чутливої» інформації. Якщо ваша система діє з етичними нормами, це зовсім не означає, що конкурент робить те ж саме.

Тому слід охороняти «чутливу» інформацію. Дієвий підхід до проблеми розробки заходів безпеки може будуватися на припущенні самого гіршого з боку конкурентів: якщо вони не обмежуються методами, які вважаються етичними, то як це може позначитися на фірмі.

Немає необхідності переконувати власників компаній, що мають інформаційні структури, що вони повинні бути надійно захищені.

На фірмі, керівництво якої серйозно думає про своє майбутнє, повинна бути створена високоефективна служба безпеці, яка забезпечить ефективний доступ до інформації і її захист.

Особливості діяльності інформаційно-аналітичного підрозділу служби безпеки фірми в кризовий період

Сьогодні актуальність цієї проблеми не викликає сумніву, тому зупинимося на ній докладніше. У кризовій ситуації залежно від динаміки, ступені зубожіння народу і відсотка його частини, що зубожіла, можуть реалізуватися погрози наступного характеру:

- загроза соціального вибуху;
- глобальне погіршення криміногенної обстановки;

- стихійне об'єднання соціальне активних, але таких, що втратили роботу людей в групи з негативним соціопсихологічним потенціалом і провокацію таких груп на антигромадські вчинки;
- посилення в більшій частині населення відчуття ненависті до приватної власності як такий зі всіма витікаючими наслідками;
- спроби відкритого або таємного розкрадання власності фірми з метою перепродажу.

нестабільності, зменшення заробітної плати, скорочення штату усередині колективу неминуче виникають відцентрові процеси. Деякі співробітники можуть впасти в депресію, деякі - озлоблюватися і почати застосовувати будь-які засоби, щоб вижити колег і залишитися в штаті.

Найбільшу небезпеку можуть представляти співробітники, готові ради додаткових доходів продавати конфіденційну інформацію конкурентам.

Тому в умовах кризи основні зусилля по збору інформації повинні бути направлені на наступні напрями:

- стан системи охоронний-пожежної сигналізації;
- стан системи інженерного захисту будівель і споруд фірми;
- внутрішній порядок і стан несення служби підрозділами фізичної охорони;
- підвищення кваліфікації охоронців і водіїв, обслуговуючих перших осіб фірми;
- вивчення морально-психологічного клімату в колективі, попередження фактів нелояльності і виявлення співробітників, що діють на шкоду фірмі в особистих корисливих інтересах.

2.3. Інформаційно – пошукова робота. Джерела інформації.

Досвід показує, що зміни і накопичення інформації відбуваються в невеликому переліку привілейованих місць, які називаються "Сімейство джерел".

Малюнок 2

Ось перелік основних сімейств джерел для будь-якого підприємства.

Клієнти - покупці клієнтів; їх інженери і кадри (перші в основному не схильні до обговорення своїх справ, тоді як останні більш схильні до розмов для створення власної значущості).

Постачальники - згідно їх діяльності (мова йде про сировину, кінцевому продукті, торгівлі майном) вони достатньо балакучі, оскільки убачають в цьому спосіб самореклами.

Банкіри - розгруповані на банківські, фінансові, біржові і кредитні установи. В основному розрізнені, але проте знають, що порадити своїм клієнтам у разі небезпеки.

Суспільні служби - рекламні агенти, фірми суспільних зв'язків, мисливці за розумом, суспільства тимчасових робіт, компанії відправлень поштових повідомлень та інші. Хоча розрізненість лежить в основі їх комерційної діяльності, вони можуть приховати свої крупні контракти.

Розподільники і агенти - незалежно від особливостей, слід брати до уваги як торговців, так і покупців.

Консультанти і експерти - незалежні або такі, що відносяться до служб підприємства фахівці, що продають свої знання у формі рад або спеціальних розробок.

Широка публікація - місцева національна і міжнародна преса.

Спеціальні видання і банки даних - їх область діяльності припускає щомісячну обробку матеріалів конфіденційних видань, що потрапляють в наукові, технічні і професійні збірки. Разом з банком даних вони складають ресурси бази даних.

Ярмарки, салони і конференції - ці демонстрації дозволяють відновити контракти з клієнтами, конкурентами і т.д., а також побачити різну продукцію, представлену на ринку.

Наукові і технічні виставки дозволяють визначити країну, що перевершує інші в своїх дослідженнях.

Адміністрація – всі нормативні зобов'язання і вимоги керівництва для майже всіх видів промисловості, комерційній і фінансовій діяльності підприємств. Вони зібрані в архівах і в більшості своїй представляють опубліковану інформацію.

Виділення необхідного джерела зі всього сімейства дозволяє в більшості випадків добратися і до інформації безпосередньо, без того, щоб проходити всі шляхи її просування. Наприклад, для нової фармацевтичної спеціальності необхідний дозвіл міністра охорони здоров'я.

Отже, завдяки описаному раніше сімейству джерел, а саме його останньому пункту - адміністрації, - застосовуючи право доступу всіх громадян до адміністративних документів, легко дізнатися специфіку продукції.

Інформація відкритого характеру

Поняття "Інформаційний ринок" з'явилося у нас на початку 90-х років 20-го століття. За кордоном це відбулося значно раніше. Наприклад, в США перше інформаційне агентство з'явилося на початку 19-го століття. Не можна сказати, що про інформацію в наший країні раніше не знали - знали і користувалися, але тільки на державному рівні. Вперше інформація з'явилася на ринку як товар в період розвитку приватного підприємництва. Починають виникати перші інформаційні агентства, випускатися комерційні довідники, з'являються перші комерційні бази даних.

В даний час інформаційний ринок України продовжує розвиватися у різних напрямах. Його основу складають: власне інформація різного вигляду і призначення, електронні операції і електронна комунікація, причому останній напрям необгрунтовано вважається головним - неначе інформація сама візьметься з нізвідки - були б тільки комунікації. Такий підхід цілком з'ясовний - поки що більшість підприємців вважають, що платити за інформацію - все одно, що платити за повітря. На жаль, державні структури, які розглядають будь-який договір на інформаційне обслуго-вування як спосіб "обналічування", "відмивання" грошей і перевіряють його "під мікроскопом", примушують споживачів інформації зміцнитися в цій думці.

Ринок власної інформації складається з декількох секторів.

1. Сектор ділової інформації, що включає біржову, фінансову, комерційну, економічну, статистичну інформацію:

- біржова і фінансова інформація включає інформацію, що надається біржами, спеціальними службами біржовій і фінансовій інформації, брокерськими компаніями, банками. Це інформація про котирування цінних паперів, валютні курси, облікові ставки, ринок товарів і капіталів, інвестиції, ціни;
- економічна і статистична інформація, що надається державними службами і компаніями, зайнятими дослідженнями і консалтингом, включає числову економічну, демографічну, соціальну інформацію у вигляді прогнозних моделей і оцінок;
- комерційна інформація. Це інформація по компаніях, фірмах, корпораціях, напрямах їх роботи і їх продукції, цінах, фінансовому стані, зв'язках, операціях, керівниках і т.п.;
- ділові новини економіки і бізнесу від спеціальних інформаційних служб.

2. Сектор інформації для фахівців, що включає науково-технічну і спеціальну інформацію, а також першоджерела:

- професійна інформація. Спеціальна інформація, властива певній професії (інформація для лікарів, юристів, викладачів, фармацевтів, інженерів і т.п.);
- науково-технічна інформація. Документальна бібліографічна, реферативна, довідкова інформація, дані в області фундаментальних і при-

кладних, природних, технічних і суспільних наук, галузей виробництва;

- доступ до першоджерел через бібліотеки і спеціалізовані служби, можливості придбання першоджерел, отримання їх по міжбібліотечному абонементу у вигляді повнорозмірних документів і мікрокопій.

3. Сектор масової і споживчої інформації, що включає новини і послуги на основі сучасних засобів телекомунікацій:

- новини і література. Інформація спеціалізованих агентств і служб новин, електронні журнали, довідники, енциклопедії;
- споживча і розважальна інформація, яка орієнтована на домашнє використання. Це - місцеві новини, погода, розклад руху транспорту, ігри, програмне забезпечення, пропозиції по обміну, покупкам і продажам, довідники готелів і ресторанів, інформація по обміну валюти, оренда машин, пропозиції по туризму, нерухомість.

Величезна кількість державних і в основному недержавних фірм і компаній працює в облас-ті інформаційного обслуговування. На світовому ринку виділилися ряд фірм і компаній, які надають своїм споживачам комплекс послуг, що охоплюють всі основні сектори інформаційного ринку.

На відміну від світового ринку ситуація на вітчизняному ринку інформації склалася достатньо непроста. Немає жодної фірми, яка готова була б надати споживачеві послуги, що охоплюють всі основні сектори ринку інформації. Серед постачальників інформації спостерігається певна спеціалізація. Велика кількість фірм надає різного роду довідкову інформацію про діяльність різних державних і комерційних структур.

Цілий ряд фірм пропонує фінансово-економічну інформацію. З'явилися і достатньо стабільно працюють фірми, що надають інформацію типу "куплю-продам", фірми, які поширюють інформацію юридичного характеру. Завдяки тому, що Україна займає одне з провідних місць в світі по виробництву "піратських" компакт-дисків і відеокасет, з'явилася величезна кількість електронних довідників на компакт-дисках по всіх сферах людської діяльності: від комп'ютерів і програмування до рад, як лікувати домашнього кота від судороги.

Велику частину інформаційного ринку займають фірми, що надають огляди преси по різним проблемам суспільного життя, а також діяльності підприємств і організацій.

З'явився попит на новий вигляд продукту - **інформаційно-аналітичні дослідження.** Підприємців (в першу чергу підприємства з іноземними інвестиціями, представництва іноземних фірм) стали цікавити аналітичні дослідження, за допомогою яких можна отримати достовірнішу картину діяльності окремої галузі промисловості або фірми. Поступово на ринку стали з'являтися аналітичні дослідження різних напрямів діяльності.

Це відстеження фінансового стану банків, так звані моніторинги, дослідження політичної обстановки в різних регіонах, аналітика розвитку тієї або іншої галузі промисловості, маркетингові звіти і багато інших аналітичних продуктів. Ці завдання частково вирішують вже згадувані інформа-ційні фірми, інформаційні підрозділи (а частіше - служби безпеки) банків, крупних комерційних структур, які в основному працюють "на себе", і спеціалізовані структури, які пропонують матеріали інформаційно-аналітичного дослідження.

Інформація закритого характеру

Цю інформацію кожна фірма збирає сама, за допомогою своєї служби безпеки, або звертається до послуг спеціалізованих фірм, що працюють в області безпеки бізнесу. Деякі фірми в своїй рекламі так прямо і пишуть: "Надаємо будь-які послуги конфіденційного характеру в рамках закону."

Збір інформації може здійснюватися наступними шляхами.

1.) " Біле шпигунство "

- збір і аналіз інформації з офіційно публікованих джерел;
- отримання інформації при відвідинах виставок, ярмарків, конференцій;
- придбання і дослідження виробів конкурентів (так звана "зворотна інженерія").

2.) " Чорне шпигунство "

- вивідування інформації, що цікавить, у фахівців конкурента, зокрема на конференціях, семінарах, виставках;
- зманювання провідних фахівців для отримання інформації, що цікавить (одночасно можуть бути досягнуті цілі відкидання конкурента на другорядні позиції, витіснення з ринку або навіть розорення конкурента);
- підкуп співробітників з ключових відділів конкурента;

- впровадження своїх агентів впливу на фірму або в близьке оточення провідних фахівців;
- викрадання креслень, документів, зразків виробів;
- негласний контроль ділової кореспонденції;
- несанкціоноване знімання інформації з комп'ютерних і телекомунікаційних мереж, магнітних і інших носіїв;
- незаконне отримання інформації у корумпованих державних чиновників, що мають відомості, що цікавлять (фінансових, митних і податкових інспекторів);
- несанкціоноване знімання інформації за допомогою технічних засобів;
- помилковий найм на роботу;
- помилкове працевлаштування свого співробітника на конкуруючу фірму;
- помилкове замовлення;
- помилкові переговори нібито з метою співпраці або придбання ліцензії і т.д.;
- шантаж і здирство.

Обробка матеріалів засобів масової інформації

Відкритий друк за традицією є самим об'ємним і найбільш використовуваним каналом отримання інформації. Сьогодні в засобах масової інформації (ЗМІ) можна отримати зведення по дуже широкому кругу питань, що цікавлять як розвідувальні, так і контррозвідувальні підрозділи Служби безпеки (СБ) підприємницького суб'єкта. Необхідно тільки правильно організувати її пошук.

Якісна робота професійних журналістів по духу близька роботі спецслужб, і це можна і потрібно максимально використовувати. Матеріали ЗМІ дозволяють зіставляти, уточнювати і забезпечувати новими подробицями дані, отримані оперативним шляхом, а також давати нові напрями для поточної інформаційно-пошукової роботи.

При плануванні роботи по аналітичній обробці преси, перш за все, треба визначитися з її метою, потім з'ясувати, що саме цікавить споживачів інформації (у тому числі і самій СБ) і лише після цього приступати до підбору джерел інформації.

Абсолютно очевидно, що для перетворення опосередкованої інформації на проблемно-орієнтований інформаційний масив, потрібно викори-

стовувати цілеспрямований підхід по активному сприйняттю інформаційних потоків, що постійно поступають. Зовсім необов'язково 24 години в добу проводити за читанням друкарської продукції - для цього цілком досить виділити півгодини свого робочого часу. Найважливіше в цій роботі - правильно підібрати джерела інформації, обробити їх з використанням принципу "ключових слів" і, нарешті, грамотно організувати сортування, класифікацію і зберігання вже відібраної інформації.

Дуже часто дані в різних джерелах багато разів дублюють один одного. Тому просте кількісне збільшення оброблюваних джерел приводить тільки до перевантаження аналітика без видимих результатів поліпшення якості його роботи. Високий рівень інформаційного шуму в оброблюваних інформаційних масивах набагато небезпечніший, ніж інформаційний голод. Так, наприклад, спеціалізовані організації для створення щоденного зведення об'ємом в одну сторінку з оцінною думкою з однієї проблеми обробляють інформаційний масив об'ємом приблизно в 7 млн. слів.

Для якісного аналізу придатності того або іншого періодичного видання досить узяти декілька його номерів за певний період, наприклад за тиждень, і скласти по рубриках список всіх опублікованих там статей.

Таким чином, з широкого спектру інформації вибирається саме той її сегмент, який найповніше співпадає з Вашими інформаційними потребами. Ця робота досить нудна і нудна, та зате з часом вона себе окупає з лишком.

Первинна обробка матеріалів ЗМІ

Працюючи з конкретною публікацією, необхідно вибирати тільки проблеми, що відповідають вашим інформаційним потребам. Ми можемо запропонувати два що принципово відрізняються, організаційних підходу до первинної обробки матеріалів ЗМІ.

Перший підхід. Використання власних можливостей по обробці ЗМІ

Всі матеріали ЗМІ, у тому числі і в електронному вигляді, що поступають на підприємство, обробляються відповідальною за це особою і, згідно розробленому класифікаторові, відповідним чином сортуються і зберігаються.

При неможливості виділення окремої штатної одиниці для роботи з пресою, співробітники служби безпеки повинні починати свій робочий день з вивчення друкарських матеріалів ЗМІ. За кожним з них закріплюється по дві-три центральних і місцевих газети; на уранішній опе-

ративці у керівництва, крім постановки завдання на день, кожен співробітник робить короткий огляд найцікавіших публікацій преси в своїй зоні відповідальності. В процесі цієї своєрідної "політінформації" відбувається обмін думками і розставляються акценти. На даних заходах кожен співробітник вибудовує для себе приблизну модель питань розвідувального плану, які він повинен буде відпрацювати "в полі".

Протягом дня на зустрічах з джерелами, в напівофіційних або неофіційних бесідах ця інформація уточнюється і перевіряється ще раз, набуваючи необхідної надійності.

Найцікавіші статті переводяться на електронні носії і вносяться до бази даних. Слід зазначити, що для зручності перекладу друкарських матеріалів в електронний вигляд доцільне застосування скануючих пристроїв, з подальшою конвертацією в текстові файли. Втім, деякі інформаційні матеріали можна безкоштовно викачати з мережі Інтернет або за відносно невисоку плату придбати в редакції видання.

Зберігання матеріалів в електронному вигляді також має певні нюанси. Матеріали можуть заноситися в базу інтегрованого банку даних (ІБД). Якщо ж організація обмежена в людських і матеріальних ресурсах і формувати власну базу даних нікому, то для роботи з об'ємними інформаційними масивами можливе використання гіпертекстових редакторів.

Другий підхід. Використання сторонніх можливостей по обробці ЗМІ.

Інформація може купуватися на стороні, чим повинні займатися спеціально виділені люди. Іноді буває так, що функції первинної обробки матеріалів ЗМІ дешевше передати стороннім особам, ніж проводити її силами власних співробітників. У первинній обробці преси значну допомогу можуть надати працівники бібліотек, які дуже дешево і достатньо професійно виконають моніторинг необхідних видань, у тому числі і іноземних.

Дайджести можуть готувати також і надомники. В даному випадку, навантаження на оперативний склад значно знижується і власний штат необхідних аналітиків стає нечисленним.

Вельми просто забезпечується і режим конспірації, щоб виконавці не мали поняття, що саме, для кого і навіщо вони роблять. У газету дається оголошення про надомну роботу, пов'язану з обробкою кореспонденції. Диспетчери на телефоні приймають заявки від охочих, зустрічаються з ними, оцінюючи їх професійну придатність. Для закріплення інтересу но-

вого співробітника до роботи служби безпеки, бажана виплата авансу і укладення договору про тимчасову роботу з можливістю його подальшого продовження. У фінансовому плані це досить економічно: якщо зникає необхідність в обробці деяких видань, то ніяких одноразових виплат по скороченню не виплачуються.

Доставка матеріалів по обробниках здійснюється кур'єром, до якого диспетчером доводиться завдання узяти газети, рознести по адресах, роз'яснити, що треба зробити і через деякий час повернути готові матеріали диспетчерові.

Кожен диспетчер працює тільки з одним обробником і одним кур'єром. Рівень конспірації при даній формі організації роботи дуже великий, так що навіть за великого бажання навряд чи хто-небудь зможе розмотати весь причинно-наслідковий ланцюжок.

По своїй спрямованості друкарські матеріали можна розділити на наступні категорії: оглядові статті, статті дискредитаційного плану, замовлені рекламні статті і статті, що розголошують комерційну таємницю.

Методологія обробки друкарських видань виділяє наступні категорії даних: базова інформація (для подальшої аналітичної обробки); поточна інформація про факти; суб'єктивно-оцінні категорії, що містять оцінки і попередження.

Читаючи статтю, необхідно проаналізувати не тільки висловлювані в ній факти, але і зрозуміти особисте відношення автора до висловлюваної проблеми.

В значній мірі цьому може допомогти приблизне уявлення про приналежність ЗМІ до конкретних фінансово-промислових угрупувань, хоча ангажована лінія часто проводиться достатньо тонко. Засоби масової інформації завжди виражають інтереси своїх господарів. Це аксіома і для нас, і для Заходу. Але, якщо західні олігархи втручаються в діяльність ЗМІ тільки в найбільш драматичні моменти, наприклад, під час воєн і виборів, то у нас преса контролюється навіть по дрібницях. Ніколи не варто перебільшувати "незалежність" журналістів - те, що ЗМІ підстроюються під "господаря", відоме всім. Матеріал, написаний журналістом і що піддався редакторській правці, може сильно відрізнятися від первинного варіанту. Але це не повинно бути приводом для відмови від роботи з інформацією.

Звичайно, дуже багато що в пресу не потрапляє або потрапляє в спотвореному вигляді. Також є вірогідність свідомої дезинформації в ході

оперативної гри, що ведеться. У будь-якому компроматі обов'язково є частка вигадки і всьому вірити не варто.

Ні для кого не секрет, що ЗМІ активно використовуються спецслужбами для легалізації інформації компрометуючого характеру. Як конкретний приклад можна привести "активну гру" ФСБ через "Московський комсомолець", про прослуховування телефонних переговорів президентської сім'ї приватним охоронним підприємством "Атол", або акцію деяких чинів прокуратури з метою дискредитації свого керівництва. Журналісти охоче йдуть на співпрацю з представниками спецслужб: хто з міркувань кар'єри, хто за гроші, хто з патріотичних або ідеологічних переконань. Іноді журналістам дійсно підсовують реальні "смажені факти", а іноді - високоякісну "дезінформа-цію". Природно, що будь-який подібний захід ретельно планується і в обов'язковому порядку узгоджується з керівництвом. На оперативному сленгу подібні заходи називаються "Контрольованим просочуванням інформації". Багато в чому ангажована наших спецслужб пояснюється нинішньою обстановкою невизначеності і нестійкості.

У період з 1991 р. по теперішній час, по різних оцінках, з органів державної безпеки з різних причин звільнилося біля 40-60 тисяч чоловік. Стіни КДБ колишнього Радянського Союзу, покинули дійсно класні фахівці, причому багато хто пішов задовго до настання пенсійного віку. Природно, що і роботу вони собі знайшли багато в чому схожу з попередньою.

Журналістика і питання економічної розвідки і контррозвідки, конкуренції, формування іміджу, престижу і рейтингових оцінок надзвичайно тісно зв'язані. Природно, що в "приватних" інформаційних війнах ЗМІ часто використовуються для розміщення матеріалів, що дискредитують діяльність конкурентів в цілях формування помилкової громадської думки, недобросовісної реклами і конкуренції або здійснення великомасштабних шахрайських операцій. В деяких випадках журналістам за публікацію "вигідної" інформації виплачується певна винагорода.

У роботі приватних спецслужб найбільш поширеною технологією легендування джерела надходження компромату - є його анонімна передача або продаж в один з численних "незалежних" інформаційно-аналітичних центрів. Після його легалізації на інформаційному ринку підключаються журналісти, які вже готують "замовлену" статтю, посилаючись на джерело, що легалізувало її. При проведенні подібних акцій

іноді має місце відверта фабрикація внутрішніх документів спецслужб і правоохоронних органів.

Також існує практика встановлення прямих контактів із ЗМІ шляхом прямого фінансування окремих видань і програм, надання ним "спонсорської" допомоги або ж безпосереднього залучення працівників ЗМІ в господарську діяльність (підрозділи по зв'язках з громадськістю).

Останнім часом широку популярність придбала легалізація матеріалів компрометуючого характеру через Інтернет. У особливо просунутих службах безпеки, крім того, що обчорнити конкурентів, існує практика добування компромату на власне керівництво з метою підготовки попереджуючих замовлених статей або передач в ЗМІ.

Якщо задатися метою і провести аналіз "замовлених" статей, то з повною упевненістю можна стверджувати, що основним двигуном "інформаційних воєн", як це не дивно, є не стільки суперечності між інтересами різних фінансово-промислових груп, скільки міжособові конфлікти їх керівництва.

Перш за все, **при аналізі інформаційних матеріалів** увага повинна концентруватися на наступних ключових моментах:

- кількість позитивних і негативних по відношенню до господарюючого суб'єкта публікацій;
- круг їх авторів, а, по можливості, і замовників;
- ступінь монополізації даної теми;
- наявні взаємозв'язки між рекламними оголошеннями конкурентів і замовленими статтями відносно того або іншого господарюючого суб'єкта;
- наявність в матеріалах збалансованої оцінки того, що відбувається, що вивчається.

Таким чином, аналіз зібраного інформаційного масиву дозволяє встановити характер взаємозв'язків між наступними основними елементами: зміст і спрямованість повідомлення, джерело повідомлення, особа журналіста, його зв'язки і контакти в ділових і політичних колах.

Основний метод, який застосовується при аналітичній обробці преси, — це зіставлення фактів, натяків, думок, версій, прізвищ, тобто різнорідній інформації по ключовому слову, прізвищу, факту.

Для якісного аналізу у ряді випадків буває достатньо смислового збігу даних з об'єктивно незалежних джерел. Як вже наголошувалося вище, "незалежність" джерел оцінюється за інформацією, що просо-

чується, про приналежність даного органу масової інформації до конкретної фінансово-промислової групи або комерційного банку.

Якщо інформація підтверджується джерелами, які належать до різних конкуруючих фінансово-промислових угрупувань, то вірогідність її достовірності велика.

Гаряча пора збору різної відкритої інформації - передвиборні кампанії в законодавчі і виконавчі органи влади. Цікавий аналіз публікацій "за і проти" різних кандидатів, фіксація факту підтримки того або іншого кандидата.

При кваліфікованому зборі і комп'ютерній обробці інформації в ІБД можна збудувати дуже цікаві схеми. Особливо чітко це можна відстежити в регіонах, де питанням оперативного легендування приділяють значно менше уваги, чим в центрі.

Так, визначення взаємозв'язків по передвиборних штабах і партійних списках дозволяє заздалегідь виявити можливий розклад груп "підтримки" того або іншого підприємницького суб'єкта в органах законодавчої або виконавчої влади.

2.4. Організація захисту інформації

Значення інформації на сучасному етапі розвитку людства безумовно важливе. Інформація сьогодні уже розглядається не тільки, як спосіб одержання різних відомостей, але й як продукт продажу. Тому проблема її збереження постала дуже гостро. А особливо це стосується інформації з обмеженим доступом, яка може бути віднесена до комерційної та державної таємниці.

Проблема захисту інформації та несанкціонованого доступу до неї прийняла антагоністичний характер в постановці, відомій із теорії гри. Стосовно проблеми захисту інформації це означає, що для її рішення необхідна не просто розробка окремих механізмів захисту, а організація цілого комплексу заходів по захисту в широкому розумінні цього питання, та. використання спеціальних засобів, механізмів і заходів з метою попередження втрати інформації.

Аналіз стану справ в області захисту інформації показує, що у розвинутих країнах склалася достатньо сформована концепція та інфраструктура захисту, основу якої складають:

– дуже розвинутий арсенал технічних засобів захисту, які створюються на промисловій основі;

– значна кількість фірм, які спеціалізуються на вирішенні питань захисту інформації;

– досить чітка система концептуальних поглядів на цю проблему;

– наявність значного практичного досвіду.

Але безумовно, як засвідчує зарубіжна преса, загрози для інформації не тільки не зменшуються, але й мають досить стійку тенденцію до зростання.

Основні концептуальні положення комплексної системи безпеки інформації організації (банку, підприємства та інших установ)

Досвід показує, що для боротьби з цією тенденцією необхідна чітка та цілеспрямована організація процесу захисту. Для цього необхідно активно залучати професійних спеціалістів, керівництво організаціями, співробітників і користувачів. Ці факти визначають підвищену значимість організаційної суті питання.

Забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, який зводиться до обґрунтування та реалізації найбільш раціональних методів, способів і шляхів удосконалення та розвитку системи захисту, безперервному контролі, виявленні її слабких місць та можливих каналів витоку інформації.

Безпека інформації може бути забезпечена тільки при комплексному використанні усього арсеналу засобів захисту у всіх структурних елементах виробничої системи і на усіх етапах обробки інформації. Найбільший ефект досягається тоді, коли усі засоби, методи та заходи об'єднуються в єдиний комплекс - комплексну систему безпеки інформації організації (КСБІ). При цьому функціонування системи захисту повинно контролюватись, поновлюватись та доповнюватись в залежності від зміни зовнішніх і внутрішніх умов.

Ніяка КСБІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і виконання ними усіх встановлених правил, направлених на захист інформації.

КСБІ можна визначити як організовану сукупність спеціальних органів,

засобів, методів і заходів, які забезпечують захист інформації на підприємстві.

З позиції системного підходу до захисту інформації установлюються такі вимоги: захист інформації повинен бути:

- неперервним,
- плановим,
- централізованим,
- цілеспрямованим,
- конкретним,
- активним,
- надійним,
- універсальним,
- комплексним.

Основні вимоги до комплексної системи безпеки інформації (КСБІ):

- чіткість визначених повноважень і прав користувачів до доступу на певні види інформації;
- надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму кількості загальних для декількох користувачів засобів захисту;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації ;
- забезпечення оцінки ступеня конфіденційності інформації;
- забезпечення контролю цілісності засобів захисту.

Надійність функціонування КСБІ також не можливе без постійного контролю за роботою її складових елементів.

Контроль комплексної системи безпеки інформації (КСБІ) - має за мету:

*- своєчасно виявити та закрити потенційні канали витоку інформації;

*- встановити відповідність змісту запланованих і проведених заходів по забезпеченню безпеки інформації (ЗБІ) системи вимогам розроблених інструкцій, пам’яток і інших документів;

*- визначити правильність організації робіт по ЗБІ і ступінь їх виконання;

*- визначити ступінь підготовки органів безпеки до виконання поставлених перед ними завдань, персоналу підприємства - з питань розробки, зберігання, обліку та роботи з документами, які вміщують конфіденційну інформацію і офісним обладнанням;

*- узагальнити досвід організації та проведення заходів з питань ЗБІ для використання його в процесі удосконалення системи безпеки;

*- перевірити організацію і результати роботи по удосконаленню системи санкціонованого доступу на підприємство, організацію допуску персоналу до конфіденційної інформації;

*- перевірити участь керівників структурних підрозділів підприємства в організації та забезпеченні виконання заходів по ЗБІ.

КСБІ як і будь-яка інша система, повинна мати певні види забезпечення, спираючись на які вона буде спроможна виконати свою цільову функцію.

З врахуванням цього КСБІ повинна мати:

**- правове забезпечення (нормативні документи);

**- організаційне забезпечення (наявність спеціальних служб: захисту документів; служби режиму, допуску та охорони; служби захисту інформації з допомогою технічних засобів та ін.);

**- апаратне забезпечення (технічні засоби захисту інформації);

**- інформаційне забезпечення (інформація для забезпечення роботи служби безпеки);

**- програмне забезпечення (програми захисту та оцінки наявності каналів витоку інформації);

**- математичне забезпечення (математичні заходи розрахунку загроз від технічних засобів розвідки, зон та норм необхідного захисту);

**- лінгвістичне забезпечення (спеціальні мовні засоби спілкування спеціалістів та користувачів в сфері захисту інформації);

**- нормативно-методичне забезпечення (методики, які забезпечують діяльність користувачів в умовах жорстких вимог захисту інформації).

КСБІ може бути охарактеризована рядом показників, які визначають її організаційну і функціональну структуру. До таких характеристик можна віднести спрямованість захисту, спосіб попередження не-

санкціонованого доступу до інформації, масштабність системи, часові характеристики впливу по ступеню активності..

Найбільш важливою характеристикою КСБІ являється направленість захисту. Розглядаються також такі напрямки захисту як правовий, організаційний і інженерно-технічний захист. Останній реалізується фізичними, апаратними та програмними засобами та математичними методами захисту.

Роль людського фактору в системі збереження державної та комерційної таємниці

Незалежно від того, на скільки добре розроблена та впроваджена КСБІ, вона в решті-решт ґрунтується на людській діяльності, в якій можливі помилки або свідомі дії, направлені на знищення інформації, або передачу її зацікавленим організаціям.

Неможна, також, не відзначити, що сьогодні, як і завжди між державами світу йде постійна боротьба за сфери своїх інтересів. І методи цієї боротьби різноманітні, починаючи від дипломатичної діяльності і закінчуючи збройними конфліктами.

Велику актуальність сьогодні мають методи "Психологічної війни".

Відомо що завданнями психологічної війни є вплив на особу, як носія інформації та як основну ланку в системах управління різноманітного призначення.

Таким чином, особа сьогодні може розглядатися як основний об'єкт атаки нетрадиційними методами ведення війни. Тому на сучасному етапі розвитку методів і засобів захисту інформації, одним із головних напрямків необхідно виділити процес виявлення і оперативної ліквідації загроз для інформації, які можуть виникати в процесі діяльності персоналу установ і організацій.

Ніяка технічна система безпеки не забезпечить надійний захист інформації, якщо хтось із персоналу установи буде свідомо здійснювати її несанкціоноване копіювання, або навмисне пошкодження.

Відомо багато методів впливу на особу з метою одержання від неї потрібної інформації, які завжди активно використовуються зацікавленими особами.

Методи впливу:

- підкуп;
- шантаж;

- погрози;
- одержання потрібної інформації при веденні звичайної розмови;
- обмін інформацією;
- переконання;
- використання психологічних методів;
- впровадження співробітником організації "своєї людини".

Усі ці факти свідчать, що для створення та надійного функціонування усіх елементів КСБІ, забезпечення кадрової безпеки організації (банку, підприємства) повинен бути створений спеціальний структурний підрозділ - служба безпеки.

Варіант організації штатної структури служби безпеки з питань захисту інформації (на прикладі банку, підприємства та інших установ)

Для організацій України, що проводять роботу з інформацією, яка становить державну таємницю, статус служб безпеки (режимно-секретних органів), їх підпорядкованість, основні обов'язки та права співробітників визначені Постановою КМУ № 609 від 4 серпня 1995 року.

Враховуючи досвід діючих служб безпеки (РСО) в установах України, а також зарубіжний і вітчизняний досвід по створенню і організації діяльності служб безпеки для недержавних установ, пропонується приблизний варіант її організаційно-штатної структури.

Служба безпеки організації повинна підпорядковуватись безпосередньо керівнику установи, а керівник служби повинен бути заступником керівника організації.

До складу служби безпеки можуть входити структурні підрозділи по збору інформації та контролю за її використанням, підрозділи технічного захисту інформації та підрозділи охорони.

Склад підрозділів служби безпеки:

1. Департамент інформації та планування:

1.1. Відділ планування та контролю:

До складу відділення входять групи:

1.1.1. Група скритого спостереження;

1.1.2. Група проведення розслідувань;

1.1.3. Група по роботі з інформаторами;

1.1.4. Група по технічному забезпеченню проведення операцій.

Основні завдання департаменту інформації та планування:

- планування роботи по забезпеченню безпеки інформації на підприємстві;
- ведення скритого спостереження за організаціями та особами;
- проведення розслідувань фактів витоку інформації, або втрат документів;
- проведення навчання персоналу організації з питань безпеки інформації;
- проведення роботи з персоналом інших організацій-конкурентів з метою їх вербування, або переходу на роботу до своєї організації;
- проводить заходи по забезпеченню безпеки інформації при використанні персональних комп'ютерів, а також при їх роботі в мережі;
- технічне забезпечення проведення різних заходів безпеки.

1.2. Інформаційний центр:

До складу інформаційного центру входять групи:

1.2.1. Група стратегічного планування;

1.2.2. Аналітична група;

1.2.3. Група по виявленню і збору відкритих і закритих публікацій (ведення діловодства);

1.2.4. Група експертів і консультантів.

Основні завдання інформаційного центру:

- проводить оцінку зовнішніх загроз для організації та розробляє комплекс заходів по їх попередженню;
- проводить збір та аналізує інформацію в середині організації;
- проводить збір літератури та нормативних документів;
- ведення діловодства;
- проводить оцінку матеріалів.

2.0. Департамент технічного захисту інформації:

До складу цього департаменту входять групи:

2.1. Група об'єктового захисту;

2.2. Група комп'ютерної безпеки;

2.3. Група безпеки зв'язку.

Основні завдання департаменту технічного захисту інформації:

- проводить встановлення та забезпечує функціонування технічних засобів охорони будівель та приміщень організації;

- ➢ - проводить заходи по забезпеченню безпеки інформації при використанні персональних комп'ютерів, а також при їх роботі в мережі;
- ➢ - проводить заходи по забезпеченню безпеки інформації при використанні засобів зв'язку (телефон, факс та ін.).

3.0. Департамент охорони:

До складу департаменту охорони входять групи:

3.1. Група охорони об'єктів;

3.2. Група особистої охорони;

3.3. Група забезпечення безпеки масових заходів;

3.4. Група охорони перевезень.

Основні завдання департаменту охорони:

- ➢ - проводить заходи по фізичній охороні та обороні будівлі та приміщень організації;
- ➢ - забезпечує особисту охорону керівництво та персоналу організації;
- ➢ - забезпечує охорону персоналу та майна організації при проведенні виставок, презентацій та інших масових заходів;
- ➢ - забезпечує охорону перевезень майна та інших цінностей організації.

Із спеціальних питань РСО також необхідно підпорядкувати відділ кадрів установи по підбору та розстановці працівників.

Структура, чисельність і склад служби безпеки організації визначається реальними фінансовими можливостями, масштабами діяльності, ступенем конфіденційності інформації. В залежності від таких факторів склад служби безпеки може бути від двох - трьох чоловік, які працюють за сув місництвом, до повномасштабної служби з розвинутою структурою. В умовах, коли основним об'єктом злочинних дій став капітал банків і комерційних підприємств, на перший план в діяльності їх особистих служб безпеки виходить інформаційно-аналітичне забезпечення, економічна розвідка та контррозвідка, а також організація оперативних заходів.

Сучасні вимоги до підготовки спеціалістів служби безпеки

Враховуючи сучасні вимоги до роботи співробітників служб безпеки (РСО) система підготовки, перепідготовки та підвищення їх кваліфікації повинна передбачати оволодіння знаннями додатково в областях:

1. Інформаційно - аналітичної роботи.
2. Методів розвідки та контррозвідки.

3. Оперативної роботи.

4. Соціальної психології та психології особистості.

5. Основи банківської справи та бухгалтерського обліку.

6. Основи менеджменту та маркетингу.

7. Цивільного та кримінального права.

Спеціаліст служби безпеки організації сьогодні повинен вміти:

1. Розробляти комплексні заходи по забезпеченню безпеки державної та комерційної таємниці організації та особистої безпеки її керівництва.

2. Здійснювати захист інформації, в тому числі і тієї, що зберігається в комп'ютерній пам'яті.

3. Використовувати технічні засоби скритого спостереження та прослуховування.

4. Протидіяти проведенню аналогічних заходів організаціями-конкурентами.

5. Розбиратися у фінансовій звітності.

6. Проводити профілактику правопорушень в організації.

7. Проводити внутрішнє розслідування випадків викрадення матеріальних цінностей, саботажу та фінансових злочинів.

8. Організовувати перевірки (в тому числі таємно) благонадійності співробітників організації.

9. Виявляти (попереджувати) випадки співробітництва працівників організації з конкурентами або кримінальними структурами.

10. Взаємодіяти із слідчими органами та міліцією при розслідуванні злочинів і інших подій.

11. Готувати документи з аналізом фінансово-економічного положення партнерів, оцінювати конкурентів і потенційних клієнтів.

12. Вирішувати конфлікти між співробітниками організації.

13. Коротко та точно висловлювати свої думки.

Наведені вище вимоги потрібно враховувати при організації підготовки, перепідготовки та підвищення кваліфікації спеціалістів системи захисту інформації.

2.5. Організація захисту комерційної таємниці

Комерційна таємниця - це відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами і іншою діяльністю підприємства, які не є державними секретами, розголошування (передача, втрата) яких може завдати збитку його інтересам .

Система заходів по захисту комерційної таємниці підприємства включає:

- організацію надійної охорони, технічного захисту приміщень, системи управління доступом;
- організацію зберігання і використання носіїв конфіденційної інформації, включаючи порядок обліку, зберігання, користування і знищення;
- організацію технічного захисту інформації; вивчення кандидатів при прийомі їх на роботу;
- навчання персоналу правилам роботи з конфіденційною інформацією, ознайомлення із заходами відповідальності за розголошування конфіденційних відомостей;
- організацію контролю за інформацією, що поступає від підприємства в зовнішні організації і ЗМІ.

Документи, що закріпляють право підприємства на комерційну таємницю

Для створення правових основ захисту конфіденційної інформації на підприємстві необхідно:

1. Внести до Статуту підприємства наступні доповнення: «Підприємство має право: визначати склад, об'єм і порядок захисту відомостей, складових комерційної таємниці, вимагати від співробітників підприємства її збереження». «Підприємство зобов'язане: забезпечити збереження комерційної таємниці».

2. Розробити "Перелік відомостей, складових комерційної таємниці підприємства".

3. Доповнити "Колективний договір" наступними вимогами:

а) Адміністрація підприємства зобов'язується: в цілях недопущення нанесення економічного збитку колективу підприємства забезпечити розробку і здійснення заходів за визначенням і захистом комерційної таємниці;

б) Трудовий колектив приймає на себе зобов'язання по дотриманню встановлених на підприємстві вимог по захисту комерційної таємниці".

4. При укладанні трудових угод (контрактів) із співробітниками підприємства внести пункт про обов'язок співробітника зберігати комерційну таємницю підприємства.

5. При узятті на посаду співробітників, робота яких буде пов'язана з конфіденційною інформацією, підписувати Зобов'язання про не розголошування комерційної таємниці.

«Перелік відомостей, що складають комерційну таємницю підприємства»

"Перелік відомостей, складових комерційної таємниці підприємства" - це зведення конкретних відомостей комерційного характеру підприємства, підлягаючий захисту. Він є юридичним документом, таким, що дає право підприємству у встановленому законодавством порядку (зокрема через судові органи) вимагати відшкодування понесених матеріальних втрат або упущеної вигоди у випадку, якщо передбачені "Переліком" відомості були розголошені, передані або втрачені особою (юридичною або фізичною), якій вони були довірені.

Склад "Переліку":

Менеджмент:

- вживані оригінальні методи управління підприємством;
- підготовка, ухвалення і виконання окремих рішень керівництва підприємства з комерційних, організаційних та інших питань;
- факти проведення, цілі, предмет і результат нарад і засідань органів управління Підприємства;
- плани розширення або згортання різних напрямів діяльності підприємства, їх техніко-економічні обгрунтування;

Фінанси:

- баланси підприємства;
- бухгалтерські книги управління;

- інформація про кругообіг засобів підприємства;
- фінансові операції підприємства, інвестиції; стан банківських рахунків;
- рівень доходів підприємства;
- боргові зобов'язання підприємства;
- стан кредиту підприємства;
- рівень заробітної плати співробітників.

Маркетинг:

- вживані підприємством оригінальні методи вивчення ринку;
- результати вивчення ринку, стани, що містяться в оцінках, і перспектив розвитку ринкової кон'юнктури;
- ринкова стратегія підприємства;
- вживані Підприємством методи збуту, способи стимулювання збуту;
- методики розрахунку, структура і рівень цін на пропоновані товари, розміри знижок;
- зведення про ефективність комерційної діяльності Підприємства;
- систематизована інформація про конкурентів;
- систематизована інформація щодо внутрішніх і зарубіжних замовників, підрядчиках, постачальниках, споживачах, покупцях, компаньйонах, спонсорах, посередниках і клієнтах;
- відомості про підготовку і результати проведення переговорів з діловими партнерами Підприємства;
- відомості, умови конфіденційності яких встановлені в договорах, контрактах, угодах і інших зобов'язаннях Підприємства.

Безпека:

- стан системи безпеки Підприємства (організація охорони, система сигналізації, режими і т.інше.);
- організація захисту комерційної таємниці Підприємства;
- інформація, складова комерційної таємниці підприємств-партнерів, передана на довірчій основі.

ЗОБОВ'ЯЗАННЯ ПРО НЕРОЗГОЛОШУВАННЯ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Я _____, поступаючи на роботу на Підприємство, протягом всієї моєї роботи і після мого звільнення, зобов'язуюся не розголошувати кому-небудь що стали мені відомими в процесі трудової діяльності зведення, складові комерційну таємницю Підприємства, а також будь-яку інформацію, що стосується:

- відомостей про фірми, що є клієнтами і діловими партнерами Підприємства;
- будь-яких відомостей щодо організаційної структури Підприємства, його кількісного і якісного складу, фінансового положення, технічного і спеціального оснащення, настановних даних, адрес, номерів телефонів керівництва Підприємства.

Зобов'язуюся також ініціативно не вступати ні у які відносини з особами з криміногенного середовища, конкуруючими організаціями, а при встановленні яких-небудь контактів з їх боку зі мною - негайно повідомляти Службу безпеці і керівництво Підприємства. Я попереджений, що у разі порушення даного зобов'язання, керівництво

Підприємства має право розірвати трудові відносини зі мною, а також прийняти інші заходи, передбачені Законом.

«_____» _____ 20__ р. _____
(підпис)

[К]

СЛУЖБОВА ЗАПИСКА

Прошу включити в "Перелік відомостей, складових комерційної таємниці підприємства" наступні відомості:

1. _____
(найменування відомостей, їх чітке формулювання)
_____

2. Гриф конфіденційності: _____
(конфіденційно, строго конфіденційно)

3. Обгрунтування для включення: _____
(новизна, конкурентоспроможність і т.д.)

4. Орієнтовна вартість відомостей:_____
(втрати, що можуть виникнути у разі втрати)

5. Орієнтовний термін дії грифа конфіденційності: _____

6. Список осіб, яким необхідно дати дозвіл на допуск до відомостей: ____
_____

Примітка: службова записка складається на кожні конкретні відомості, які відносяться до категорії "комерційна таємниця".

«_____» _____ 20_____ р.

_____
(підпис керівника підрозділу)

Зразок НАКАЗУ по підприємству щодо захисту комерційної таємниці

НАКАЗ № _____

«____» _____ 20_____ р.

Про введення в дію Положення про комерційну таємницю Підприємства і правила її збереження, і створення Комісії з питань комерційної таємниці

Керуючись чинним законодавством України (Росії, Білорусі...) в цілях захисту, складових комерційної таємниці підприємства

НАКАЗУЮ:

1. Ввести в дію Положення про комерційну таємницю підприємства і правила її збереження.

2. Створити Комісію, що постійно діє, з питань комерційної таємниці в складі:
Голова Комісії _____
Члени Комісії _____

3. Комісії приступити до роботи з "_____"_____ 20___ р.

4. Покласти на Комісію наступні завдання:

· збір пропозицій від підрозділів підприємства про відомості, які можуть бути віднесені до комерційної таємниці підприємства і підлягають захисту від витоку;

· вивчення пропозицій, що поступають, їх узагальнення і оцінка, систематизація і розробка "Переліку відомостей, складових комерційну таємницю підприємства".

5. Керівникам структурних підрозділів підприємства з урахуванням Положення "Про комерційну таємницю Підприємства і правила її збереження" провести оцінку комерційних та інших планів, структури цін, оглядів ринку, внутрішньої інформації і т.інше. до «_____» _____ 20___ р. представити в комісію пропозиції зі встановленої форми ("Службова записка") про внесення до "Переліку" відомостей, які доцільно вважати конфіденційними.

6. Голові Комісії: забезпечити контроль за своєчасним надходженням матеріалів від керівників структурних підрозділів; представити "Перелік" мені на затвердження до «_____» _____ ц.р.

7. _____ у десятиденний термін ознайомити з діючим наказом членів комісії і керівників структурних підрозділів (за списком), що беруть участь в підготовці відомостей для "Переліку".

Керівник Підприємства

Положення (типове) про комерційну таємницю підприємства і правила її збереження

І. Загальні положення.

1.1. Комерційну таємницю підприємства складають відомості, пов'язані з економічною, управлінською і іншою діяльністю підприємства, розголошування (передача, втрата) яких може завдати збитку його інтересам, спричинити прямі економічні втрати або упущену вигоду.

1.2. Відомості, складові комерційної таємниці, отримані в ході господарської діяльності Підприємства, належать власне підприємству.

1.3. Діюче Положення визначає основи захисту комерційної таємниці підприємства. Вимоги і правила, викладені, в Положенні обов'язкові для виконання всіма підрозділами підприємства.

ІІ. Заходи по захисту комерційної таємниці.

2.1. Організація і проведення заходів щодо захисту комерційної таємниці здійснюється Службою безпеки Підприємства.

2.2. При організації захисту конфіденційної інформації на паперових і магнітних носіях переслідуються наступні завдання:

- виключити інстанції походження носіїв конфіденційної інформації і дій з ними;
- попередити не обгрунтоване ознайомлення з конфіденційною інформацією, а також втрату і розкрадання такої інформації.

Перше з вказаних завдань досягається за рахунок раціональної організації руху носіїв конфіденційної інформації по рівнях управління підприємства, друге завдання - за рахунок диференційованого підходу до видачі дозволів на доступ до конфіденційних відомостей відповідно до виробничої необхідності.

ІІІ. Методика виділення відомостей, складових комерційної таємниці.

3.1. Право кваліфікувати інформацію, як комерційну таємницю підприємства, надається керівникам структурних підрозділів підприємства.

3.2. При виділенні відомостей, складових комерційної таємниці підприємства, необхідно керуватися наступними критеріями:

3.2.1. Недостатні заходи щодо захисту інформації можуть нанести таку ж утрату підприємству, як і надмірне засекречування інформації.

3.2.2. "Ноу-хау" в області менеджменту і маркетингу, зведення про новий вигляд товарів, інша інформація, що захищається, повинні мати дійсну або потенційну цінність.

3.2.3. Не потребують додаткового захисту і не можуть бути віднесені до комерційної таємниці підприємства відомості, захищені патентами і авторським правом, а також що є державними секретами.

3.2.4. Відповідно до Ухвали КМ. України від 9 серпня 1993 року № 611 "Про перелік відомостей, що не є комерційною таємницею" до комерційної таємниці не відносяться:

- засновницькі документи, документи, що дозволяють займатися підприємницькою і господарською діяльністю і її окремими видами;
- інформація по всіх встановлених формах державної звітності;
- дані, необхідні для перевірки начислення і сплати податків і інших обов'язкових платежів;
- відомості про чисельність і склад тих, що працюють, їх заробітній платі в цілому і по професіях і посадах, а також наявності вільних робочих місць;
- документи про сплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, не дотримання безпечних умов праці, реалізацію продукції, яка завдає шкоди здоров'ю, а також інші порушення законодавства України і розміри заподіяного при цьому збитку;
- документи про платоспроможність;
- зведення про участь посадових осіб підприємства в кооперативах, малих підприємствах, союзах, об'єднаннях і інших організаціях, що займаються підприємницькою діяльністю;
- відомості, що підлягають оголошенню відповідно до діючого законодавства.

IV. Грифи конфіденційності.

4.1. Раціональний розподіл носіїв конфіденційних відомостей по рівням управління базується на класифікації вказаних носіїв по ступеню важливості інформації, що міститься в них, тобто на віднесенні конфіденційної інформації до однієї з вказаних нижче груп:

1 група - носії, що містять зведення по принциповим питаннях діяльності підприємства;

2 група - носії, що містять відомості по поточних питаннях комерційної і господарської діяльності Підприємства;

3 група - носії, що містять зведення по приватних питаннях діяльності підприємства.

4.2. Відповідно групам конфіденційної інформації на підприємстві вводяться наступні грифи конфіденційності: “Строго конфіденційно ” - 1 група, “Конфіденційно” - 2 група і “Службова інформація ” - 3 група.

4.2.1. Гриф “Строго конфіденційно” [СК] привласнюється тільки тим носіям, пропажа яких може привести до дуже крупних матеріальних втрат або припиненню діяльності підприємства. Документи з цим грифом повинні бути виконані в одиничних екземплярах; доступ до них можуть мати тільки керівник підприємства, засновники і Рада директорів.

4.2.2. Гриф “Конфіденційно” [К] виставляється на носіях, зміст яких не повинен стати відомим (за поряд виключень) особам, що не входять в апарат управління (адміністрацію) підприємства. Цей гриф доцільно привласнювати документам суто внутрішнього користування і що містять інформацію, яка може бути використована конкурентами або кримінальними елементами для нанесення серйозного збитку підприємству. Документи з цим грифом адресуються в рамках прав і обов’язків посадовим особам підприємства для ухвалення рішень.

4.2.3. Гриф “Службова інформація” [СІ] застосовується для всіх носіїв, що містять службову інформацію. Пропажа цих носіїв не може нанести істотну матеріальну утрату підприємству, але, проте, не бажана. Для роботи з документами [СІ] не вимагається спеціального дозволу. До-

кументи з цим грифом можуть без особливої обмовки передаватися клієнтам, контрагентам і діловим партнерам, але не повинні передаватися дійсним і потенційним конкурентам підприємства.

4.3. Привласнення грифа конфіденційності документу, а також зняття (пониження) грифа після закінчення певного терміну проводиться керівниками структурних підрозділів підприємства, про що повідомляється Служба безпеки підприємства.

V. Допуск до конфіденційних документів.

5.1. Для виключення несанкціонованого ознайомлення з конфіденційною інформацією на підприємстві використовуються два види дозволів на доступ:

- адресна резолюція керівника підприємства і його заступників (в рамках повноважень) на документах, що містять конфіденційну інформацію;
- список посадових осіб підприємства, що мають право доступу до документів з грифом "Конфіденційно", а також наділених правом надання доступу до працівників безпосередньо підлеглих підрозділів і працівників суміжних підрозділів по клопотанню їх керівників.

VI. Відповідальність за розголошування конфіденційної інформації.

6.1. Співробітники підприємства зобов'язані строго берегти комерційну таємницю, що стала їм відомою в процесі трудової діяльності на підприємстві.

6.2. Відповідальність за організацію збереження комерційної таємниці несуть керівники підрозділів підприємства. Неправомірне ознайомлення виконавців з конфіденційною інформацією, розглядається як розголошування комерційної таємниці і спричиняє за собою відповідну відповідальність.

6.3. У разі умисного розголошування (передачі, витоки) конфіденційної інформації, унаслідок чого підприємству нанесений матеріальний або інший збиток, співробітник притягується до відповідаль-

ності, передбаченої трудовим, адміністративним, цивільним або кримінальним законодавством.

“Затверджую”
Керівник підприємства

«____» _____ 20 ____ р.

ІНСТРУКЦІЯ
По організації і веденню на підприємстві конфіденційного діловодства.

І. Загальні положення.

1.1. Організація конфіденційного діловодства - це сукупність сил, а також засобів, правил, методів і прийомів діяльності по діловодству і режимному забезпеченню комерційних секретів підприємства, пов’язаних із створенням, зберіганням і використанням документів, в яких міститься комерційна таємниця.

1.2. Справжня інструкція розроблена з урахуванням положень “Єдиної державної системи документального забезпечення управлінь”, Гостів, що діють, на організаційно – розпорядливу документацію, а також практики ведення секретного де¯діловодство в Збройних Силах.

1.3. Конфіденційне діловодство проводить Служба безпеки (СБ) підприємства після створення необхідних умов для ведення цієї роботи: виділення окремого приміщення, обладнаного системою охоронно-пожежної сигналізації, необхідної кількості сейфів і металевих шаф для зберігання документів.

1.4. У разі тимчасової відсутності співробітника СБ, що відповідає за ведення конфіденційного діловодства (хвороба, відпустка, відрядження і т.інше.), його обов’язки виконує інший співробітник по вказівці начальника СБ.

1.5. Виділення інформації, складової комерційної таємниці, проводиться відповідно до “Методики виділення інформації, складової комерційної таємниці підприємства і визначення грифів конфіденційності цієї інформації”.

II. Облік конфіденційних документів.

2.1. Складання і оформлення документів.

2.1.1. Конфіденційні документи (з грифами [СК] і [К]) складаються і печатаються в строго обмеженій кількості екземплярів, які визначає керівник підрозділу, що складає ці документи.

2.1.2. Підготовлені документи разом з чернетками (якщо вони виконані не в спеціальних врахованих зошитах) передаються в СБ підприємства для реєстрації. Браковані або віддруковані зайві документи також здаються в СБ для знищення по акту.

2.1.3. Зняття копій і виробництво виписок з конфіденційних документів проводиться з дозволу керівника структурного підрозділу підприємства. Оформлення копій і виписок здійснюється по правилах, прийнятих для конфіденційних документів.

2.2. Конфіденційні документи повинні оформлятися по спеціальним правилам .

2.2.1. На обкладинці кожного конфіденційного документа повинні міститися наступні відомості:

- в правому верхньому кутку ставиться гриф конфіденційності документа;
- під ним проставляється інвентарний номер даного документу, який реєструється в Книзі обліку конфіденційних документів.

Гриф конфіденційності дублюються на титульному листі документа, що робиться на випадок, якщо обкладинка документа буде відірвана.

2.2.2. Листи конфіденційного документа нумеруються і прошиваються міцною ниткою, кінці якої заклеюються цигарковим папером. На

цигарковому папері ставиться відтиснення гербової печаті Підприємства або спеціально виготовленого друку “Для документів”.

2.2.3. На останньому листі документа робиться наступний напис:

У цьому документі пронумеровано і прошнуровано _____ листів.

_____
(підпис відповідальної особи)

2.2.4. Кожен додаток до конфіденційного документа повинен мати:
- найменування застосування;
- гриф конфіденційності;
- номери і кількість екземплярів, що додаються;
- самостійну порядкову нумерацію листів і сторінок.

2.2.5. У разі, коли конфіденційні документи виконані на окремих листах, прошнурувати які не представляється можливим, вони вкладаються в теку, в яку вклеюється реєстр, що враховує наявність в теці листів. Кожен листок отримує гриф конфіденційності і інвентарний номер, який наголошується в реєстрі формою:

Інвентарний №	Гриф конфіденційності	Назва	Дата вилучення	Підпис

Сама тека отримує гриф не нижче за найбільш конфіденційний в ній листок і власний інвентарний номер, який враховується в Книзі обліку конфіденційних документів.

2.2.6. Для роботи над чернетками конфіденційних документів співробітникам підприємства видаються спеціальні враховані зошити. Вони оформляються і враховуються таким же чином, як і конфіденційні документи.

2.3, Всі конфіденційні документи Підприємства підлягають обов'язковому обліку в Книзі обліку конфіденційних документів.

2.3.1. "Книга" складається з наступних розділів:

№ п/п	Інв.№	Назва	Гриф конф.	Кіль-ть листів	Дата отримання	Підпис	Дата вилучення	Підпис

2.3.2. "Книга" розділяється на дві частини: одна частина визначається для обліку документів [СК], інша - для документів [К]. При збільшенні кількості і руху конфіденційних документів на Підприємстві (створенні розвиненої мережі філій), СБ заводить дві "Книги" для обліку документів [СК] і [К] відповідно.

2.3.3. "Книга" повинна мати гриф [К]. Це пов'язано з тим, що тільки згадка або фіксація тільки назви документів з грифом [СК] вже само по собі містить конфіденційну інформацію.

2.3.4. У "Книзі" забороняється робити стирання або виправлення із застосуванням рідини, що коректує. У разі внесення невірного запису вона закреслюється одним штрихом, а внизу сторінки "Книги", де були проведені виправлення, робиться надпис: "Закреслене не читати", і ставиться підпис співробітника СБ, що відповідає за конфіденційне діловодство. Якщо виникає необхідність виправити вже наявний запис, старий запис закреслюється одним штрихом, над нею пишуться виправлення, а внизу сторінки "Книги" робиться запис: "Виправленому вірити", і ставиться підпис.

III. Видача конфіденційних документів.

3.1. Конфіденційні документи повинні видаватися тільки особам, що мають право на роботу з ними: - згідно адресної резолюції керівника підприємства і його заступників (в рамках повноважень) на документах;

- згідно списку посадових осіб підприємства, що мають право доступу до документам з грифом [К], а також наділених правом надання дос-

тупу до працівників безпосередньо підлеглих підрозділів і працівників суміжних підрозділів по клопотанню їх керівників.

3.2. Доставка конфіденційних документів віддаленим користувачам проводиться нарочним. Пересилка конфіденційних документів поштою здійснюється тільки з дозволу керівника підприємства, керівників структурних підрозділів або начальника СБ замовленим або цінним поштовим відправленням.

IV. Зберігання конфіденційних документів.

4.1. Конфіденційні документи зберігається в сейфах окремо від іншої документації.

4.2. Робочі документи з грифом [СК] зберігаються в сейфах керівництва підприємства або в СБ.

4.3. Робочі документи з грифом [К] зберігаються в приміщеннях структурних підрозділів Підприємства за наявності в них умов, що забезпечують збереження даних носіїв. Якщо ці можливості відсутні, документи передаються на зберігання в СБ.

4.4. Всі конфіденційні документи, які вже не використовуються, але повинні зберігатися в перебігу певного часу, передаються на зберігання в СБ. Терміни зберігання конкретних документів визначаються керівником підприємства і керівниками структурних підрозділів, про що робиться відповідна відмітка на матеріалах.

V. Знищення конфіденційних документів.

5.1. Знищенню підлягають документи і справи, що втратили практичне значення і що не мають комерційної або історичної цінності для підприємства.

5.2. Документальні матеріали знищуються на підставі рішення Комісії з питань комерційної таємниці.

5.3. Поділа і документи з минулими термінами зберігання, чернетки конфіденціальних документів, а також відпрацьований копіювальний папір, фарбувальна стрічка машин, що пишуть, і матричних принтерів знищується в робочому порядку працівниками СБ.

5.4. Знищення документальних матеріалів проводиться шляхом спалювання або роздрібнення на спеціальних машинах.

VI. Контроль за конфіденційним документообігом.

6.1. Конфіденційний документообіг підприємства знаходиться під постійним контролем СБ.

6.2. Контроль здійснюється трьох видів:

- поточний;
- у вигляді планових перевірок (квартальних і річних);
- у вигляді непланових перевірок (проводяться по вказівці начальника СБ при виникненні підозр про просочування інформації або у разі втрати конфіденційних документів).

6.3. Співробітники СБ зобов'язані вимагати від виконавців забезпечення встановленого справжньою Інструкцією порядку обліку, зберігання, розмноження і користування конфіденційними документами.

Перевірки стану режиму поводження з конфіденційними документами проводяться на робочих місцях виконавців.

6.4. Про результати контролю і проведені перевірки начальник СБ докладає керівникові підприємства.

Розділ 3.

Оперативно-профілактична робота по захисту інформації

Програмна анотація

3.1. Загальні поняття про оперативну обстановку,

- фактори, що впливають на оперативну обстановку.

3.2. Ймовірні шляхи дій агентури супротивника,

- загально-типові форми і методи дій агентури супротивника,
- секрети охороняють люди,
- напрямки забезпечення охорони секретів підприємства
- заходи по створенню системи захисту об'єктів.

3.3. Загальні методи по забезпеченню власної інформаційної безпеки.

- властиві помилки вітчизняних бізнесменів,
- загальні рекомендації по забезпеченню Вашої життєдіяльності,
- висновки по безпеці витоку конфіденційної інформації.

3.1. Загальні поняття про оперативну обстановку

У попередніх розділах, автори давали поняття про розвідувальну і контррозвідувальну діяльність спецслужб та оперативно-розшукову – правоохоронних органів – частково порушувалося питання, пов'язане з визначенням поняття такої категорії безпекознавства як „оперативна обстановка" [1].

Проте ознайомлення з багатьма науковими та фаховими публікаціями останнього часу, в яких інші автори висвітлюють умови, в котрих забезпечується безпека суб'єктів господарювання в підприємницькій сфері, засвідчило те, що не всі вони достатньо чітко розуміють сутність, зміст і сферу застосування категорії „оперативна обстановка", особливо у прикладних дослідженнях та під час підготовки текстів нормативних документів. Складається ситуація, коли співробітники державних спецслужб більш обізнані, частіше застосовують термін „оперативна обстановка", а їхні колеги із служб безпеки недержавних суб'єктів господарювання намагаються „конструювати велосипед", що виглядає не зовсім коректно щодо сталих понятійних категорій безпекознавства.

Не зважаючи на те, що в загальний науковий обіг автором вже було введено таке специфічне фахове поняття як „оперативна обстановка", виникла нагальна потреба більш детально висвітлити теоретичні та прикладні аспекти зазначеної категорії, особливості її застосування у нормотворчій діяльності. Для розкриття практичного значення цього поняття доцільно стисло нагадати основні теоретичні положення про оперативну обстановку.

По-перше, первісне поняття „обстановка" – це, насамперед, стан, характер умов і сукупність чинників виробництва; значення, місце і роль інтересів політичних сил, військових, представників ділових кіл, громадських лідерів у конкурентній боротьбі; розстановка політичних, економічних і військово-стратегічних сил на міжнародній арені, в регіоні, в окремій державі, організації тощо на певний момент часу.

Оперативна обстановка – це складне поняття, котре складається із елементів економічної, політичної, ідеологічної, соціальної, криміногенної та інших видів обстановок в тому чи іншому суспільстві або регіоні. Зазначені види обстановок у даному випадку виступають як чинники, основоформуючі передумови оперативної обстановки. Опера-

тивна обстановка визначає відповідні умови та сукупність чинників, що на них впливають, в яких діють:

- правоохоронні органи, спецслужби (розвідка і контррозвідка), дипломатичні служби, інші державні органи, відповідальні за правопорядок, громадську, державну, економічну, інформаційну та інші види національної безпеки, захист життєво важливих інтересів суспільства та оборону держави;
- представники організованих злочинних угруповань, латентних структур;
- учасники міжцивілізаційної, міжнародної і регіональної економічної, науково-технічної, політичної, ідеологічної, військово-стратегічної конкуренції; релігійного та міжетнічного протистояння;
- інші учасники міжнародних і внутрідержавних суспільних відносин.

Всі учасники відносин, що відбуваються в певній оперативній обстановці, поділяються на генеральних і виконавчих суб'єктів. У теорії міжнародних відносин до генеральних суб'єктів відносять держави, міжнародні, державні та недержавні організації, латентні співтовариства і навіть фізичних осіб з високим міжнародним авторитетом [2].

На формування характерних рис оперативної обстановки в сфері забезпечення безпеки держави, суспільства, людини і громадянина всередині країни та на міжнародній арені активно впливають внутрішні та зовнішні чинники у вигляді діяльності головних (генеральних) суб'єктів в особі вищих посадових осіб держав, державних органів влади та управління, транснаціональних фінансово-промислових, валютно-банківських об'єднань, економічних і науково-виробничих корпорацій, керівників і впливових активістів таємних транснаціональних елітарних співтовариств та підпорядкованих ним виконавчих суб'єктів в особі структур зовнішньополітичних відомств (дипломатичні служби посольств, консульств, військових місій, культурних, науково-технічних аташе, мовно-культурних центрів), загальнонаціональних державних спецслужб, спецслужб недержавних приватних підприємницьких структур (від транснаціональних корпорацій до середніх і дрібних), правоохоронних органів, зокрема кримінальної, податкової поліції тощо [3].

У даному випадку всі перелічені учасники відносин є суб'єктами правовідносин, тому що вони мають відповідну юридичну правоздатність і дієздатність. Зазначені суб'єкти діють у межах відповідних правових принципів і норм. Що стосується держав, міжнародних організацій та

інших об'єднань, утворених державами на підставі міждержавних і міжнародних договорів чи угод, а також вищих посадових осіб держав та зазначених владних міжнародних організацій, то перелічені юридичні особи як такі, що поряд з юридичною правоздатністю та дієздатністю мають додатково й відповідні владні (публічні) повноваження щодо законотворчої і правозастосовної діяльності, – визначаються суб'єктами міжнародного і національного публічного (владного) права. Одночасно в цій сфері оперують також декласовані, маргінальні, латентні елементи, тобто різного спрямування і потужності мафіозні структури, організовані злочинні угруповання, екстремістські та терористичні організації, окремі впливові злочинні авторитети, а також різні види латентних об'єднань тощо.

Серед всіх учасників міжнародних і внутрідержавних суспільних відносин особливе місце займають так звані виконавчі суб'єкти (насамперед спецслужби, правоохоронні органи), які забезпечують сприятливі та безпечні умови реалізації генеральними суб'єктами стратегічних і поточних завдань щодо досягнення визначених цілей, захисту національних чи корпоративних інтересів, реалізації перспектив стратегії розвитку націй, народів, держав, міждержавних об'єднань, транснаціональних угруповань, цивілізацій.

Як зазначалося вище, основними складовими елементами оперативної обстановки визначаються економічна, політична, ідеологічна, соціальна, криміногенна, релігійно-конфесійна, міжетнічна, міжнаціональна та інші види обстановок в тому чи іншому суспільстві, державі, регіоні, чи в міжнародному, глобальному масштабі. В залежності від рівня актуалізації, зазначені види обстановок у даному випадку виступають як чинники, як основоформуючі передумови оперативної обстановки.

У випадку забезпечення безпеки господарюючих суб'єктів, особливо у сфері підприємницької діяльності, де за законами бізнесу головними понятійними категоріями, а також рушійними елементами, є „прибуток" і „конкуренція", – активно оперують як загальнонаціональні державні спецслужби, так і спецслужби підприємницьких структур (від транснаціональних корпорацій до середніх і малих), інших різновидів сучасних неурядових організацій, рухів, об'єднань.

Проте, фахівці з безпекознавства головними чинниками визнають політичну (в тому числі й міжнародну), ідеологічну, економічну та

соціальну обстановки, котрі негативно або позитивно впливають на розвиток інших видів безпеки.

Політична обстановка в оперативній обстановці позначається специфікою вияву особливостей політичної боротьби. Політична боротьба – це продукт, засіб і форма виявлення суспільних відносин, котрих немає поза діяльністю людини, тобто поза боротьбою людини за свої права, пріоритети, владу, інтереси та потреби. У зв'язку із цим політична боротьба репрезентує глобальне явище соціальної реальності, котре уособлює в собі взаємозв'язок і діалектичну взаємодію своєрідних форм виявлення економічних, соціальних, ідеологічних та політичних відносин, тобто первинних основоформуючих елементів, котрі дозволяють визначати характеристики основних ознак загальної оперативної обстановки.

Політичні відносини безпосередньо реалізуються в політичній діяльності, боротьбі суб'єктів політики, існування без яких об'єктивно неможливе. Нині принципи вищості політики над економікою вимагають вирішення виробничих завдань через суспільні інтереси, а не містечкових, тобто під кутом зору підпорядкування цих завдань загальнонаціональним цілям економічної політики в межах стратегічного розвитку нації, держави. Якщо провідні політичні сили не додержуються цих принципів і виробничий процес вступає у протиріччя з політичними інтересами, тобто домінує над ними – це беззаперечно тягне за собою невиправдані ускладнення в політичній обстановці в регіоні, світі чи на конкретному об'єкті безпекознавчого захисту.

Відмінна ознака політичної обстановки визначається конкурентною взаємодією з приводу влади між суб'єктами міжнародних і внутрідержавних правовідносин взагалі, державами та окремими особами, політичними партіями, рухами, угрупованнями. Зазначені учасники правовідносин за своїм правовим статусом, повноваженнями і відношенням до влади поділяються на суб'єктів міжнародного публічного (владного) або приватного (невладного) права. Аналогічним чином вони розподіляються в межах національного права – суб'єкти владного (адміністративного, кримінального, господарського тощо) і приватного (цивільного, сімейного, трудового, соціального забезпечення тощо) права. Це означає, зокрема, що:

- якщо окремі особи, групи населення порушують закони, постанови, рішення, прийняті вищими органами влади держави, то вони в певній мірі впливають на політичну обстановку;

- висловлювана незгода з існуючим політичним курсом правлячої еліти держави або окремими її суб'єктами, а також політичними силами, об'єднаними в партіях чи рухах тощо не дозволяє політичній системі певного суб'єкта міжнародного чи національного права (насамперед, держави) здійснювати свої владні функції в сфері внутрішньої і зовнішньої політики.

Ідеологічна обстановка в оперативній обстановці тісно пов'язана з політичною обстановкою. Ідеологічна обстановка фахівцями з безпекознавства визначається як процес виникнення, розвитку та вирішення протиріч у свідомості людей, що постійно провокуються впливом антагоністичних відмінностей уявлень про спосіб організації суспільства і напрямки суспільного розвитку, котрі пропагуються правлячими елітами держав, а також іншими суб'єктами міжнародного права та реальними діями окремих фізичних осіб із числа відповідальних партійних, громадських і державних діячів або їхніх активістів (прихильників) як носіїв цих ідеологій та осіб як носіїв відмінної ідеології, спрямованих проти ідеології конкурента.

Матеріальною основою ідеологічної діяльності є система економічних відносин, котрі утворені певними групами політичних сил (класами, кланами), носіями відповідних ідеологій. Таким чином, провідними виразниками ідеологій нині стали партії, котрі, репрезентуючи авангард тієї чи іншої групи політичних сил (класу, клану), організують боротьбу зі своїми ідеологічними чи політичними супротивниками, об'єднаними в партії, рухи, секти та інші угруповання. Звідси, ідеологічна обстановка залежить від:

- економічної і політичної обстановки;
- системи поглядів, ідей;
- політико-правових, моральних, етичних, релігійних, філософських уподобань окремих лідерів, керівників, інших представників певних політичних сил (класів, кланів), партій, рухів, угруповань, а також їхньої практичної діяльності.

Наявність протиріччя між поглядами та діями є відмінною рисою ідеологічної обстановки, тому що ступінь розповсюдження ідей, ідеалів у розшарованому на певні політичні сили (класи, клани) суспільстві не обмежується лише формуванням свідомості в населення. Вона передбачає поєднання цього протиріччя з практичною діяльністю, з вираженням мотивів соціальної поведінки. Ідеології формуються і передбачаються для

поширення не лише для виховування певного прошарку чи всіх політичних сил суспільства, навіть не для окремих особистостей, а для забезпечення умов виникнення і посилення мобілізуючих стимулів, спрямованих на реалізацію певних інтересів. У зв'язку із цим, як правило, ідеї завжди компрометували себе, якщо вони віддалялися від інтересів. Механізми виникнення протиріччя:

1.) На першому етапі виникає економічна обстановка в економічній боротьбі. 2.) На другому – економічна обстановка формує політичні (класові, групові, кланові, корпоративні) інтереси, свідомість – з цього моменту зароджуються передумови для ідеологічної обстановки. 3.) На третьому – розвиток боротьби, усвідомлення суб'єктом необхідності боротьби за владу створює передумови для виникнення політичної обстановки.

Економічна обстановка в оперативній обстановці – це, насамперед, сукупність відносин і протиріч, котрі виникають у конкретних місцях застосування праці. Вони властиві певній групі осіб, певному процесу виробництва і певному часу. Іншими словами, економічна обстановка – це сукупність умов і стимулюючих чинників протікання процесу вирішення протиріч у трудовій діяльності, антагоністичного чи неантагоністичного характеру. В цьому процесі завжди взаємодіють дві сторони: роботодавець – найманий робітник, керівник – підлеглий тощо.

Соціальна обстановка в оперативній обстановці як чинник має велике значення для суспільної безпеки в контексті політичної та ідеологічної боротьби. У зв'язку із цим необхідно розуміти, що первинними елементами соціальної обстановки визначаються:

- дії груп особистостей,
- умови виробництва (відносини між людьми в умовах певного способу виробництва, добування коштів на життя),
- інтереси певних політичних сил, партій, рухів чи угруповань тощо.

Для вирішення проблеми оцінки, аналізу, прогнозування і моделювання ситуації в сфері безпеки в тому чи іншому регіоні взагалі та економічної діяльності конкретного суб'єкта господарювання: фірми, підприємства, кредитно-банківської чи іншої недержавної підприємницької структури, зокрема – важливо проводити постійний моніторинг, відбір інформації щодо змін у показниках характеристик, котрі визначають відхилення параметрів від запланованого стану потенціалів головних регіональних і світових гравців, а також характеру

їхнього впливу на відносини між суб'єктами економічної конкуренції, – держав і сучасних могутніх транснаціональних наддержавних об'єднань, – на предмет виявлення ознак певної напруженості: збройних конфліктів, революцій, контрреволюцій та інших соціально-економічний потрясінь як природного походження, так і штучного, створеного спецслужбами іноземних конкурентів, супротивників та ворогів. Потенціали держави чи іншого учасника міжнародних відносин, у даному випадку в економічній сфері, визначаються наступним:

- економічні можливості;
- засоби: матеріальні, людські запаси, джерела їх оновлення та поповнення;
- науково-технічні досягнення, винаходи, котрі надають суб'єкту міжнародної (політичної, економічної, воєнно-стратегічної, науково-технічної тощо) конкуренції, якісно нові засоби боротьби;
- кількісні та якісні показники сил, засобів, їхня дислокація в певний період;
- досконаліть їхньої організаційної структури та ефективність управління ними, мобілізаційні можливості, мобільність в розгортанні та інші складові елементи протиборства.

Кожна із сторін забезпечує безпеку своїх потенціалів за допомогою системи державних заходів і системи спеціальних органів, котрі реалізують зазначені державні заходи. Наявність потенціалів у сторін породжує потребу забезпечити безпеку і зберегти їх у таємниці від конкурентів, супротивників чи партнерів. З цією метою використовуються як легальні, так і нелегальні форми, методи, прийоми та засоби протиборства.

Так, приміром, сучасні переможці в „холодній війні" США і держави НАТО для досягнення переваг прагнуть проникнути до потенціалів, насамперед, всіх посткомуністичних чи інших держав, віднесених ними до списку країн із недружніми, тоталітарними чи недемократичними режимами, з метою контролю над суспільствами цих держав або, в разі крайньої необхідності, підірвати їхній потенціал, як вже це було зроблено проти СРСР, Югославії, Афганістану, Іраку, та інше.

У даному випадку основним об'єктом спрямувань таємних операцій іноземних конкурентів є політична влада, тому що встановлення контролю над економічним, оборонним, науково-технічним, іншими потенціалами вирішує частково проблему домінування, і тому відіграє вторинну роль під час проведення таємних операцій. Завдання щодо

визначених потенціалів є похідними, тому що їхня реалізація не досягає кінцевого результату – стратегічної мети у геостратегічній, геополітичній і геоекономічній конкуренції в сучасному глобалізованому світі. Встановлення повного контролю над конкурентом неможливе без встановлення над ним політичної влади.

Як свідчить практика сучасної політичної боротьби, ідеологічної та економічної конкуренції, а такої практика втручання іноземних сил у внутрішні справи України [5], особливо останніх 2-3 років, – лише через встановлення політичного контролю досягається кінцева мета – поширення влади через кадрову політику на всі інші потенціали держави-об'єкта розвідувальних спрямувань – систему державного управління, економіку, оборонну, систему безпеки, зовнішню політику, науку, освіту, соціальну сферу, ЗМІ тощо. Як наслідок – кардинальна зміна не лише внутрішніх, а й, у першу чергу, зовнішніх орієнтирів у діяльності держави. Така постійна зміна політичних сил у владі та орієнтирів розвитку суспільства призводить у кінцевому рахунку до дестабілізації суспільних відносин і руйнації державного механізму як основи забезпечення безпеки суверенітету і державності.

Оскільки реальні дані щодо потенціалів, як правило, всіляко приховуються і вони складають частину державної таємниці, тому проникнення до них можливе лише за допомогою таємних, негласних, прихованих, спеціальних форм і методів, а їхній підрив – нелегальними та легальними угрупованнями. Тобто шляхом проведення конкурентами комплексних оперативних заходів і таємних операцій. Аналогічна ситуація складається і навколо провідних недержавних суб'єктів господарювання: виробничих об'єднань, корпорацій, фінансово-банківських і комерційних структур.

Аналіз політичної боротьби свідчить, що кожна із протидіючих сторін покладає надії на підтримку окремих осіб, груп людей, які поділяють погляди протидіючої сторони та в принципі можуть виконувати завдання щодо проникнення до таємних потенціалів або здійснити їхній підрив. Мотиви у зазначених осіб можуть бути як свідомі, так і несвідомі. У зв'язку із цим фахівці називають їх потенційними агентами супротивника, тому що подібні особи об'єктивно мають можливості надавати допомогу супротивнику.

Особливості розвитку оперативної обстановки створюють умови для існування протиріччя між можливостями супротивника встановлювати агентурні відносини з особами, які мають доступ до потенціалів, що

охороняються, і здатністю держави (або національного значення недержавних суб'єктів господарювання) – об'єкту розвідувальних посягань протидіяти цим спробам. Вирішення цього протиріччя можна здійснити через:

- встановлення супротивником контактів із потенційним агентом шляхом його вербування;
- створення агентурних позицій в контррозвідці та розвідці, службах безпеки як державних, так і недержавних структур, в середовищі підвищеної вербувальної активності супротивника з метою стеження за процесами і проведення заходів щодо підстави своїх джерел на вербування.

У цьому випадку в оперативній обстановці відбувається зміщення центру ваги протиборства із легальної сфери в нелегальну. Це обумовлюється об'єктивними тенденціями розвитку оперативної обстановки, котрі полягають у виникненні відносин з моменту вербування за наступною моделлю: супротивник – агент – потенціал (таємниця), котрі опосередковані людською діяльністю, а в агентурних відносинах соціальні зв'язки виступають у вигляді:

- інформації щодо потенціалу, розстановки сил і засобів у нелегальній боротьбі;
- ознак впливу, підриву, конкретного результату у вигляді шкоди державі, іншому суб'єкту міжнародних правовідносин або національного значення недержавних суб'єктів господарювання.

Таким чином, **оперативна обстановка** – це стан, характер умов та сукупність чинників процесу вирішення протиріч у певний момент часу і на конкретній території при проникненні супротивника до таємних потенціалів держави (чи окремого суб'єкта господарювання) або в підриві потенціалів. Точніше – оперативна обстановка репрезентує певний момент політичної боротьби на конкретній території, де виникають дві конкуруючі сторони: держава (системи держави) або національного значення недержавних суб'єктів господарювання як об'єктів захисту від небезпек, ризиків, викликів і загроз – і супротивник. У результаті антагоністичної взаємодії цих двох елементів, які стають джерелом, виникає і розвивається оперативна обстановка.

Аналіз і безпекознавча оцінка має завданням визначити де, коли, яким чином супротивник прагне досягти переваг, тобто завчасно передбачити, спрогнозувати діяльність супротивника в умовах невизначеності та

відсутності достатніх знань про нього. Вирішення зазначеного вище завдання має бути комплексним:

По-перше, розглядаючи оперативну обстановку під кутом зору загального, особливого і одиночного, доцільно визнати, що:

- політична боротьба, виступаючи як загальне явище соціальної дійсності в окремо взятій державі та в цілому на міжнародному рівні, характеризується певною розстановкою політичних сил, партіями, ідеологіями, потенціалами тощо;
- особливі моменти в політичній боротьбі виражаються через процеси розвитку політичної, економічної та ідеологічної обстановок;
- одиничне (неповторне) виражається через оперативну обстановку, котра має в собі моменти загального і особливого.

Звідси виходить, що оперативна обстановка є вихідним моментом політичної боротьби у широкому значенні, у вузькому значенні – економічної конкуренції в сфері господарювання, її одиничним проявом. Вона завжди конкретна, одинична в певному просторі та часі.

По-друге, в кожному конкретному випадку необхідно виділяти причини (чинники) виникнення характерних рис оперативної обстановки. Якщо виходити із посилання, що вона є процесом, необхідно визнати наступне:

- будь-яка діяльність, котра утворюється із економічних, політичних та ідеологічних процесів тощо, не може виробляти продукт своєї діяльності миттєво;
- тому потребується певний час для виникнення цих процесів;
- загострення оперативної обстановки розвивається, досягає свого апогею, потім поступово спадає і зникає.

Відповідно до теорії циклічності розвитку процесів оперативна обстановка має наступні форми градації стану:

Виникнення (зародження) – це момент зародження, з одного боку, протиріч (чинників), тобто економічної, політичної, ідеологічної, інших видів обстановок. Зазначені протиріччя між державою і супротивником розвиваються до рівня певної системи через потребу в супротивника проникнути до таємного потенціалу або його підірвати, а у держави (або національного значення недержавних суб'єктів господарювання) – об'єкта розвідувальних спрямувань – організувати контррозвідувальну протидію цим зазіханням і захист наявного в нього потенціалу.

Розвиток – це продовження процесу поглиблення протиріч в економічній, політичній, ідеологічній, в інших актуальних обстановках. Цей процес характеризується виявленням додатково нових чинників і умов в оперативній обстановці. Вони начебто накопичуються в процесах економічної, політичної, ідеологічної, соціальної та інших обстановок, досягаючи певної критичної межи.

Криза – це момент максимального загострення протиріч, тобто певний апогей процесу розвитку, під час котрої відбувається заміна влади, зміна економічної основи держави, нелегальні сили та засоби супротивника переходять на легальне положення, виникає так звана „революційна" або „контрреволюційна" ситуація.

Спад – це момент природного чи штучного вирішення протиріч в оперативній обстановці. Правлячі кола, отримавши інформацію про виникнення або про розвиток оперативної обстановки, використовують протиріччя на свою користь, впливаючи на визначені спецслужбами чинники та умови таким чином, щоб випередити супротивника в його діях. Спад оперативної обстановки є найбільш стабільним її утворенням, властивим їй протягом досить тривалого часу.

Будь-яке явище завжди підпорядковується закону причинності, в тому числі й оперативна обстановка, тому всяка її зміна потребує пізнання причин виникнення тієї чи іншої обставини. Якщо причини стають відомі спецслужбам, вони мають змогу спрогнозувати сутність і характер їхніх наслідків. Проте, необхідно враховувати, що визначення оперативної обстановки за схемою „потенціал служби безпеки (контррозвідки) – супротивник – середовище – об'єкти забезпечення безпеки" не завжди точно віддзеркалює сутність явищ.

Для аналізу, насамперед контррозвідувальної, оцінки необхідно брати більш ширший спектр показників тому, що чинники, котрі виступають як причини (рушійна сила процесів оперативної обстановки) дозволяють виділити низку різносторонніх закономірних наслідків. Багаточисельні наслідки кожного із чинників саме і є тими умовами, котрі мають нині обов'язково враховуватися аналітиками в довідках про оперативну обстановку.

Підсумовуючи вище викладені теоретичні міркування, вважається доцільним рекомендувати керівникам служб безпеки недержавних суб'єктів господарювання розробляти відповідну „Типову концепцію без-

пеки суб'єкта господарської діяльності", використовуючи викладені авторами положення щодо оперативної обстановки.

Така „Типова концепція" має починатися розділом „Організаційно-правові заходи забезпечення безпеки підприємства", в якому викладаються результати безпекознавчого аналізу та оцінки небезпек, ризиків, викликів і загроз.

Зокрема, у підрозділі „Загальні положення" визначається, що концепція безпеки підприємницької структури розроблена у відповідності до вимог:

- Статуту підприємства, Установчого договору, Колективного трудового договору;
- Господарського кодексу України, Цивільного кодексу України, Кодексу про адміністративні правопорушення України, Кримінального кодексу України;
- Законів України „Про державну реєстрацію юридичних осіб та фізичних осіб-підприємців" від 3 березня 2005 р., „Про ліцензування певних видів господарської діяльності" від 1.06.2000 р.;
- Постанови КМ України від 10 серпня 1993 р. № 615 „Про заходи щодо вдосконалення охорони об'єктів державної та інших форм власності";
- Наказів Державного комітету України з питань регуляторної політики та підприємництва, Міністерства внутрішніх справ України від 21 березня 2001 р. № 53/213 „Про затвердження Ліцензійних умов провадження господарської діяльності з надання послуг, пов'язаних з охороною державної та іншої власності, надання послуг з охорони громадян"; від 21 березня 2001 р. № 53/213 „Про затвердження Ліцензійних умов провадження господарської діяльності з виробництва, ремонту вогнепальної зброї та боєприпасів до неї, холодної зброї, пневматичної зброї калібру понад 4,5 міліметра і швидкістю польоту кулі понад 100 метрів на секунду, торгівлі вогнепальною зброєю та боєприпасами до неї, холодною зброєю, пневматичною зброєю калібру понад 4,5 міліметра і швидкістю польоту кулі понад 100 метрів на секунду; Ліцензійних умов провадження господарської діяльності з виробництва спеціальних засобів, заряджених речовинами сльозоточивої та дратівної дії, індивідуального захисту, активної оборони";
- Наказу МВС України 25.11.2003 р. № 1429 про затвердження „Інструкції із здійснення підрозділами ДСО заходів майнової та

особистої безпеки громадян з використанням технічних засобів охорони";

- інших законодавчих і нормативних актів України, що регламентують питання безпеки підприємств, діяльності правоохоронних органів.

Про ймовірні шляхи дій агентури супротивника будемо розглядати в наступному розділі книги.

3.2. Ймовірні шляхи дій агентури супротивника

Перехід країн СНД від планового господарювання до ринкового, виникнення численних приватних підприємств, зниження ролі державного регулювання в різних сферах економічного життя - все це веде до різкого посилення конкуренції між виробниками товарів і послуг. Історичний досвід свідчить, що в цілому конкуренція сприяє розвитку продуктивних сил і прогресу суспільних відносин. Однак лише тоді, коли вона здійснюється в цивілізованих формах. Саме в цьому випадку перевага одержує той із суперників, чия стратегія спрямована на підвищення якості пропонованих товарів і послуг, зниження цін на них, надання додаткових пільг споживачам. У той же час протиборство між конкурентами може відбуватися з використанням нецивілізованих, несумлінних і навіть незаконних засобів і методів. У таких ситуаціях уперед виривається не той, хто краще працює, хто більше піклується про споживача, а нахабний 'деляга' або злочинець.

На жаль, у цей час у країнах СНД і Балтії одержали широке поширення саме нецивілізовані форми конкурентної боротьби. Живильний ґрунт для них створюють специфічні умови пострадянського економічного простору: загальна низька культура підприємницької діяльності, незавершеність процесу формування ринкових відносин, відсутність або неефективність багатьох законодавчих і нормативних актів, економічна нестабільність (інфляція, безробіття, неплатежі), відсутність розгалуженої системи державних органів і громадських організацій для боротьби з нецивілізованою, несумлінною й незаконною конкуренцією.

Основний принцип конкуренції зі знаком "мінус" полягає в прагненні зміцнити своє становище за рахунок ослаблення позицій конкурентів (аж до їхнього повного витиснення) або за рахунок обману

споживачів, або шляхом сполучення того й іншого. Нецивілізована конкуренція здійснюється у формі економічного шпигунства, корупції, брехливої реклами, компрометації окремих співробітників і фірм у цілому, фальсифікації й підробки продукції конкурентів, маніпулювання з діловою звітністю для одержання різних фінансових вигід й, нарешті, за допомогою прямого обману, грабежу, завдання матеріальних збитків, психологічного й фізичного придушення (аж до вбивства).

Поговоримо про економічне шпигунство та ймовірні шляхи проникнення агентури супротивника. Відповідно до оцінок американських експертів, втрати фірм і корпорацій у США, обумовлені розкраданням конфіденційної інформації, становили на початку 90-х років близько 40 мільярдів доларів! Тим часом, опитування російських підприємців, проведений в середині 90-х років московським центром по вивченню проблем несумлінної конкуренції, показав що тільки 37% з них розуміють необхідність цілеспрямованого захисту своїх комерційних секретів.

Конфіденційною вважається така інформація, розголошення якої може завдати шкоди інтересам фірми. Вона розділяється на інформацію обмеженого доступу й на секретну. До першого ставляться ті відомості, розголошення яких заподіює збиток тактичним інтересам, таким, як зрив конкретного контракту, зниження відсотка прибутку від угоди, ускладнення умов виконання окремої угоди, накладення фінансових або інших санкцій з боку партнера й інші в тім же дусі. Розголошення секретної інформації завдає серйозної шкоди стратегічним інтересам фірми, може поставити під погрозу саме її існування надалі . Її становлять відомості, ознайомлення з якими дозволяє конкурентам, неперебірливим у засобах, підірвати репутацію фірми в очах партнерів, заподіяти їй значний фінансовий збиток, привести до конфлікту з державними органами, поставити в залежність від кримінальних структур.

Визначення ступеня конфіденційності службової інформації здійснює, як правило, керівництво фірми. Однак у кожному разі до такій ставляться:

- Статутні документи фірми;
- Зведені валютні й карбованцеві звіти по фінансовій діяльності фірми (щомісячні, квартальні, річні, за кілька років);
- Кредитні договори з банками;

- Договори купівлі й продажу, починаючи від певної суми (для дрібної фірми це може бути тисяча доларів, для великої - двадцять п'ять або сто тисяч "зелених", або їхній еквівалент у рублях);
- Відомості про перспективні ринки збуту, джерелах засобів або сировини, товарах, про вигідних партнерів;
- Будь-яка інформація, надана партнерами, якщо за її розголошення передбачені штрафні санкції.

Конфіденційна інформація існує, як правило, у матеріальній формі. Це зразки продукції або товарів, різні документи, креслення, плани, схеми, аналітичні огляди, моделі, каталоги, довідники, зафіксовані на папері, фотографіях і слайдах, у дискетах ПЭВМ.

Нерозуміння вітчизняними бізнесменами значення мір по захисту конфіденційної інформації є однією із причин небажання західних партнерів мати з ними справа. Вони приїжджають, дивляться на те, як вирішуються проблему охорони офісів, комерційних секретів, посміхаються, підписують протоколи про наміри - і не роблять ні кроку далі. Вони розуміють, що все вкладене ними буде або розграбовано, або використане з мінімальною ефективністю. А головне - украдуть їхні комерційні таємниці.

Тим часом, у Західній Європі й у США втрата 20% конфіденційної інформації приводить до руйнування фірми протягом одного місяця.

Письмове опитування (анкетування) 250 бізнесменів, проведений улітку 94 роки показав, що найбільш типовими формами й методами економічного шпигунства вони вважають:

1) - підкуп або шантаж співробітників фірми - 43% відповідей;

2) - знімання інформації з ПЭВМ спецтехнікою (проникнення в бази даних, копіювання, і т.д.)- 42%;

3) - копіювання (розкрадання) документів, креслень, експериментальних і товарних зразків - 10%;

4) - прослуховування телефонних розмов та різне підслуховування розмов; - 5%.

5) - інші способи – 5%

Цікаво зрівняти результати цього опитування з думкою групи експертів країн Загального ринку (середина 90-х років) про форми й методи несанкціонованого доступу до комерційних секретів конкуруючих фірм, ми бачимо схожі показники:

1) підкуп або шантаж співробітників фірми, впровадження туди своїх агентів - 42% відповідей;

2) знімання інформації з ПЭВМ спецтехнікою - 35%;

3) копіювання (розкрадання) документів, креслень, товарних зразків та інше - 13%;

4) прослуховування й підслуховування - 5%;

5) інші способи - 5%.

Як бачимо, висновки обох груп зацікавлених осіб разюче близькі один одному. Що ж стосується умов, що сприяють витоку комерційних секретів фірм, то опитування 2-х тисяч респондентів у п'ятьох містах України, проведений центром по вивченню проблем несумлінної конкуренції в середині 90-х років, дав наступні результати:

- балакучість співробітників, особливо у зв'язку із споживанням алкоголю й у дружніх компаніях - 35% відповідей;
- прагнення співробітників заробити гроші будь-яким способом, за принципом "гроші не пахнуть" - 27%;
- відсутність служби безпеки фірми - 23%;
- "совкова" звичка співробітників "ділитися передовим (і іншим) досвідом", давати ради стороннім - 5%;
- безконтрольне використання інформаційних і копіювальних засобів на фірмі - 4%;
- психологічні конфлікти між співробітниками, між співробітниками й керівництвом, набір випадкових людей, що жадають "продатися" або "помститися" - 6%.

Загально-типові форми й методи дій агентури супротивника

1. Підкуп. Це найпростіший й ефективний спосіб одержання конфіденційної інформації. Зрозуміло, він вимагає деякої попередньої роботи для з'ясування ступеня поінформованості тих або інших співробітників фірми в її справах. Крім того, підкуп звичайно здійснюється через посередників, тому необхідною умовою є збір інформації про їх: треба точно знати, кому дати гроші, скільки, коли, через кого й за що. Однак всі витрати такого роду з лишком перекриваються однією важливою обставиною - працівникові фірми не потрібно переборювати фізичні й технічні перешкоди для проникнення в її секрети.

Виходить, залишається лише одне: знайти власників потрібної інформації, незадоволених своїм просуванням по службі, заробітком, ха-

рактером відносин з керівниками, що гостро бідують у грошах або просто жадібних, готових заради наживи на будь-яке зрадництво. Відома смутна статистика (дані Інтерполу), відповідно до якої 25% фірми, що служить, готові продати її секрети в будь-який час кому завгодно, 50% ідуть на це залежно від обставин і тільки 25% є патріотами даного підприємства.

Одним з видів підкупу є переманювання коштовних фахівців фірми до себе заради наступного оволодіння їхніми знаннями. Історія конкурентної боротьби повна подібних прикладів.

Для тих 50% співробітників, які йдуть на співробітництво з конкурентами залежно від обставин, необхідні "обставини" нерідко створюють через шантаж.

2. Шантаж буває двох видів. У першому випадку людини ловлять на "гачок", загрожуючи зрадити розголосу компрометуючі його відомості. У другому випадку, йому просто загрожують заходами фізичного впливу (підірвемо автомобіль, спалимо дачу, викрадемо дитини, зґвалтуємо дочку або дружину, залякаємо старих батьків і т.д., засобів у злочинців багато).

3. Впровадження "своїх" людей до складу персоналу конкуруючої фірми теж представляє розповсюджений й ефективний спосіб шпигунства. Для впровадження є два шляхи:

- Перший - коли агент виступає під власним прізвищем і працює відповідно до наявної в нього професією.
- Другий - коли він працевлаштовується по підроблених документах, під прикриттям "легенди".

Впровадження власних агентур до конкурентів більше складний метод, чим звичайний підкуп або шантаж, але на відміну від завербованих інформаторів, свій агент набагато надійніше й ефективні-ше як джерело конфіденційної інформації.

4. Конфіденційні помічники. Залежно від ступеня цінності інформатора будуються й відносини між сторонами, що співробітничають. Чим він важливіше, тим більше дотримується мір конспірації. Зокрема , зустрічі з ним маскуються під побутові контакти, відбуваються на конспіративних квартирах або в громадських місцях, через схованки й навіть за допомогою технічних засобів. Спілкування з менш коштовними людьми може носити звичайний характер. При цьому сторони особливо не піклуються про свою безпеку. Так що вибіркове сховане спостереження

за власними співробітниками може дати керівникові фірми (через його оперативних співробітників) досить цікаві відомості для міркувань.

5. Знімання інформації з ПЭВМ здійснюється багатьма способами. Перелічимо їх:

- розкрадання носіїв інформації (дискет, магнітних дисків, перфокарт);
- копіювання програмної інформації з носіїв;
- читання залишених без догляду роздруківок програм;
- читання інформації з екрана сторонньою особою (під час відображення її законним користувачем або при його відсутності);
- підключення до ПЭВМ спеціальних апаратних засобів, що забезпечують доступ до інформації;
- використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань ПЭВМ (відомо, що за допомогою спрямованої антени таке перехоплення можливе у відношенні ПЭВМ у металевому корпусі на відстанях до 200 метрів, а в пластмасовому - до одного кілометра);
- несанкціонований доступ програм до інформації, або розшифровка програмної зашифрованої інформації.

Останній спосіб називається "електронний грабіж", а людей, що займаються їм, називають "хакерами". Даний вид злочинів найпоширеніший там, де є комп'ютерні мережі в масштабі фірми, організації, населеного пункту або регіону.

По оцінках швейцарських експертів, щорічні втрати, пов'язані із крадіжкою інформації з ЕОМ, становлять нині в Західній Європі близько 60 мільярдів доларів у рік (!). Усього один приклад у цьому зв'язку: фірма "Британська енциклопедія" порушила кримінальну справу проти трьох операторів свого комп'ютерного центра, обвинувативши їх у тім, що вони скопіювали й продали стороннім особам імена й адреси приблизно трьохсот тисяч замовників.

6. Спостереження теж дає коштовну конфіденційну інформацію, особливо якщо воно сполучено з копіюванням документації, креслень, зразків продукції й т.д. У принципі, процес спостереження складний, тому що вимагає значних витрат сил, часу й засобів. Тому його ведуть, як правило, вибірково, це значить, у певнім місці, у певний час, спеціально підготовленими людьми й за допомогою технічних засобів.

Наприклад, волоконно-оптична система типу РК-1715 має кабель довжиною до двох метрів. Вона дозволяє проникати в приміщення через замкові щілини, кабельні й опалювальні уведення, вентиляційні шахти, фальшиві стелі й інші отвори. Кут огляду системи - 65°, фокусування - від 10 км до нескінченності… . Працює при слабкому висвітленні. З її допомогою можна читати й фотографувати документи на столах, замітки в настільних календарях, настінні таблиці й діаграми, зчитувати інформацію з дисплеїв.

Взагалі фотографування застосовується в промисловому шпигунстві досить широко. Фотозйомка здійснюється за допомогою сучасних апаратур при денному висвітленні й уночі, на сверхблизькій відстані й на видаленні до декількох кілометрів, у видимому світлі й в інфрачерво-ному діапазоні (в останньому випадку можна виявити виправлення, підробки, а також прочитати текст на обгорілих документах). Сучасні шпигунські фотоапарати вражають уяву. Так, відомі телеоб'єктиви розміром усього із сірникову коробку, однак чітко знімають друкований текст на відстанях до 100 метрів! А мініатюрна фотокамера в наручних годинниках (типу РК-420) дозволяє робити 7 кадрів на одній касеті з відстані від одного метра й далі, - без наведення на різкість, установки витримки, діафрагми й інших тонкостей.

Більшу небезпеку в плані економічного шпигунства представляють люди, що володіють фотографічною зоровою пам'яттю. Їм досить одного погляду, щоб охопити значний зміст, запам'я-тати й відтворити його практично без перекручувань. Особливо легко це вдається фахівцям з розвідки, яким досить лише натяку, щоб вони зрозуміти основний зміст тексту (креслення, розробки). От приклад. Конкуруюча фірма послала на перегляд моделей одягу свого конкурента групу модельєрів, кожний з яких спеціалізувався на якій-небудь одній деталі демонстрованих моделей: на рукаві, комірі, спинці й т.д. В умовах найсуворішої заборони на фотографування, відеозйомку, замальовки й навіть на розмови (щоб виключити диктування на магнітофон) вони запам'ятали кожний свої деталі. Потім у себе на фірмі вони відновили в малюнках усе, що бачили, по кожній моделі!

6. Прослуховування й підслуховування по своїй значимості перебувають на останнім місці серед основних форм і методів одержання конфіденційної інформації. Це й зрозуміло, тут інформа-ція збирається випадковим образом, безсистемно, до 90-95% відсотків її становлять ви-

словлення не представляють ніякого інтересу для конкурентів. Крім того, потрібно багато часу для аналізу цієї інформації. Проте, даний метод використається дуже широко, внаслідок своєї простоти.

Підслуховування телефонних переговорів найпоширеніше. Воно здійснюється такими способами:

- За рахунок мікрофонного ефекту телефонного апарата;
- Шляхом контактного підключення до лінії зв'язку;
- Шляхом безконтактного підключення до телефонної лінії;
- За допомогою телефонних радіо закладок, жучків, клопів та інше;
- За рахунок так називаного високочастотного "нав'язування".

Важливо відзначити, що підслухувати можна не тільки стаціонарні телефонні лінії, але й берегово-ри по радіотелефоні, у тому числі в системах стільникового зв'язку. Все залежить від того, який спосіб прослуховування й за допомогою яких апаратур здійснюється. Крім того, підслухувати можна розмови в приміщеннях або в автомашинах за допомогою попередньо встановлених радіо закладок ("жучків", "клопів") або мініатюрних магнітофонів. Ті й інші - комуфлюється під різні предмети, деталі одягу, побутові прилади, освітлювальні арматури й т.д. Наприклад, відомий підслуховующий пристрій, змонтований у вигляді стінного цвяха має три модифікації.

Загалом кажучи, кількість моделей що підслухують і записують мову наявних на ринку технічних пристроїв,, не піддається ніякому обліку. З їхньою допомогою можна приймати, підсилювати, очищати й записувати будь-які розмови (у тому числі шепотіння або під звук води, що ллється із крана) досить чітко й надійно.

Існують і більше складні методи підслуховування, наприклад, за допомогою лазерного випромі-нення шибок у тім приміщенні, де ведуться "цікаві" розмови. Або шляхом спрямованого радіовип-ромінювання, що змушує "відгукуватися й говорити" деталі в радіоприймачах, телевізорах, настінних годинниках й іншій побутовій техніці. Однак подібні методи вимагають наявності складної й досить дорогої техніки, тому застосовують їх в економічному шпигунстві досить рідко.

У конкурентно-ринкових відносинах виникає маса проблем, пов'язаних із забезпеченням схоронності конфіденційної (комерційної) інформації. Адже бізнес тісно пов'язаний з одержанням, нагромадженням, зберіганням, обробкою й використанням різноманітних масивів інформації. І якщо інформація являє певну цінність, то факт таємного одержан-

ня її конкурентом приносить йому певний доход, послабляючи, тим самим, можливості тих, хто протистоїть йому на ринку.

Можливо також внесення певних змін до складу інформації, чинене в корисливих цілях, наприклад, з метою дезінформації. Однак внесення змін важко здійснювати, тому що для правдо- подібності її треба погоджувати із загальним ходом подій за часом, місцю, меті й змісту, що вимагає глибокого знання обстановки в конкуруючій фірмі. Тому більше розповсюдженою й небезпечною метою є знищення накопичених інформаційних масивів або програмних продуктів у документальній і магнітній формі.

Таким чином, зловмисник може **переслідувати три мети:**

1) - одержати необхідну інформацію в обсязі, необхідному для конкурентної боротьби;

2) - внести зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;

3) - завдати шкоди конкурентові шляхом знищення комерційно коштовної інформації.

Повний обсяг відомостей про діяльності конкурента неможливо одержати тільки яким-небудь одним з можливих способів доступу до інформації. Тому чим більшими розвідувальними можливіс-тями володіє зловмисник, тим більших успіхів він може домогтися в конкурентній боротьбі. І взагалі, на успіх може розраховувати тільки той, хто швидше й повніше збирає необхідну інформацію (у тому числі конфіденційну), переробляє її й приймає правильні рішення. Основні шляхи й методи її одержання ми тут розглянули. Тепер познайомимося з методами захисту конфіденційної інформації, у широкому змісті цього терміна - “захист”.

Секрети охороняють люди

Світовий досвід захисту комерційних секретів фірм показує, що успіх у цій справі дає тільки комплексний підхід, що поєднує адміністративно-організаційні та соціально-психологічні міри. До числа перших ставляться:

1) Наявність служби безпеки, що відповідає, серед іншого, за схоронність комерційних секретів;

2) Організація спеціального діловодства, що включає в себе класифікацію документів по ступені й строкам їхньої таємності, що відповідає облік, зберігання, використання, знищення або розсекречення;

3) Оптимальне обмеження числа осіб, що присвячують у комерційні секрети фірми, дотримання ними правил користування конфіденційною інформацією;

4) Наявність охорони на всіх об'єктах фірми, підтримка там, де це необхідно, пропускного й внутрішньо-об'єктного режиму;

5) Проведення мір, що виключають (або істотно утрудняють) використання конкурентами технічних засобів перехоплення або знімання інформації з її носіїв.

Загальна система мір по захисту комерційної інформації

Розробляючи систему мір по захисту комерційних секретів фірми, співробітник, відповідальний за безпеку, повинен зробити наступне:

1. Визначити (разом з керівництвом й експертами) перелік відомостей, що становлять комерційну таємницю. У цьому переліку відзначити найціннішу інформацію, що вимагає особливої охорони;

2. Установити строки, протягом яких ті або інші відомості є секретними (або закритими для сторонніх осіб);

3. Виділити категорії носіїв секретної й закритої інформації - конкретних співробітників; документи, вироби, матеріали; технічні засоби зберігання, обробки, тиражування й передачі інформації; фізичні випромінювання;

4. Виділити із просторової зони і матеріалізувати комерційну таємницю в носіях інформації (місця й час роботи, переговорів, ярмарків, виставок, нарад і т.д.);

5. Скласти схему робіт з конкретними відомостями, матеріалізованими в конкретних носіях, із прив'язкою цих захисних заходів до місця й часу.

Всі елементи системи захисту комерційних секретів фірми необхідно постійно аналізувати для оцінки її фактичного стану, виявлення недоліків і порушень. Такий аналіз повинен також містити в собі моделювання ймовірних каналів витоку інформації, можливих прийомів і способів її несанкціонованого одержання конкурентами.

Ймовірні канали витоку конфіденційної інформації

Закордонні фахівці до числа найбільш імовірних каналів витоку конфіденційної інформації відносять наступні:

- спільну діяльність із іншими фірмами;
- проведення переговорів;

- екскурсії й відвідування фірми;
- рекламу, публікації в пресі, інтерв'ю для преси;
- консультації фахівців з боку, що одержують доступ до документації й виробничої діяльності фірми;
- фіктивні запити про можливості роботи у фірмі, висновку з нею угод, здійснення спільної діяльності;
- розсилання окремим співробітникам фірми різних анкет і запитальників під маркою наукових або маркетингових досліджень;
- приватні бесіди зі співробітниками фірми, нав'язування їм незапланованих дискусій по тимі або інших проблемах.

Додаткові заходи безпеки по витоку інформації

Аналіз системи захисту комерційних секретів, моделювання ймовірних погроз дозволяє намічати, при необхідності - додаткові заходи безпеки. При цьому ступінь їхньої доцільності визначається досить просто: витрати на забезпечення належної таємності повинні бути істотно менше, ніж можливий економічний збиток.

Однак, як образно виразився один експерт, "ступінь надійності будь-якого шифру визначається не його складністю, а непідкупністю шифрувальника". Іншими словами, ключовими фігурами систем захисту комерційних секретів є співробітники фірм. Причому не тільки ті, які працюють із закритою інформацією (хоча дана категорія в першу чергу). Рядовий співробітник, що не має досту-пу до комерційної таємниці, теж може надати допомогу конкурентам у проведенні електронного шпигунства, забезпечити умови для розкрадання носіїв інформації, для вивідування, зняття копій.

На думку закордонних фахівців, (про що ми писали вище), імовірність витоку відомостей, що становлять комерційну таємницю, при проведенні таких дій, як підкуп, шантаж, переманювання співробітників фірми, впровадження своїх агентів становить 43%; одержання відомостей шляхом їхнього вивідування в співробітників - 24%. Таким чином, персонал фірми, з одного боку, є найважливішим ресурсом підприємницької діяльності, а з другого -, окремі співробітники в силу різних обставин можуть стати джерелом великих втрат і навіть банкрутства фірми. Саме тому організаційні й адміністративні із захисту конфіденційної інформації необхідно сполучати із соціально-психологічними мірами.

Серед соціально-психологічних мір захисту можна виділити **два основних напрямки:**

Перший – це правильний підбор і розміщення кадрів,

Другий - це використання матеріальних і моральних стимулів.

Західні фахівці з підприємницької безпеки вважають, що від правильного підбора, розміщення й стимулювання персоналу, схоронність фірмових секретів залежить, як мінімум, на 80%!

У поняття підбора входить, насамперед , вивчення професійної придатності кандидатів у співробітники й вибір серед них найбільш підходящих. Для правильного підбора визначальну роль грає всебічна інформація про особистості кандидата і його попередньої діяльності. Тому актуальна є проблема збору такої інформації, про ці та інші методи ми детально описували в 1 томі книги.

Основні методи збору інформації

У наш час використаються наступні основні методи збору інформації: вивчення документів й інших письмових джерел; бесіди й опитування; тестування; спостереження в процесі роботи, спілкування, відпочинку; соціально-психологічний тренінг.

Вивчення письмових джерел і документів (у тому числі таких, як характеристики, рекомендації, відкликання, подання, атестації, накази, доповідні записки, публікації в пресі) традиційно є основним способом знайомства з особистістю й діловими якостями нових кандидатів на роботу. Однак цей спосіб найменш інформативний. Саме його мають на увазі, коли говорять: “у чужу душу не залізеш”. (Тим часом, сучасна психологічна наука дозволяє залізти в будь-яку душу з такою ефективністю, що дослідники довідаються про людину навіть те, чого він сам про себе не знає. Ці дані дозволяють прогнозувати поводження досліджуваної людини в різних ситуаціях з 99% точністю! Тому ми пропонуємо читачеві знову повернутися до 1 тому книги. Значно більше важливої інформації можна почерпнути з бесід й опитувань.

Бесіда – це одержання відомостей від самого кандидата в співробітники.

Опитування – одержання усних відомостей про нього від інших осіб. За рубежем збір відомостей про кандидатів на роботу шляхом усного опитування становить значну частину замовлень приватних детективних агентств. У СНД поки що цим способом як правило зневажають, віддаючи перевагу особистій бесіді керівника (або кадровика) з кандидатом. До

подібній до бесіди, за рідкісним винятком, спеціально не готуються, програма її не складається, а тому й ефект її незначний. Усе зводиться до горезвісного "загальному враженню", коли бізнесмен, поняття не має про психологію і її методи, зовнішні дані людини приймає за прояв його схованих якостей.

Спостереження за працівником може здійснюватися під час стажування або іспитового терміну, у штучно створених (спеціально для перевірки) ділових ситуаціях, у процесі роботи. Дуже інформативне вивчення найближчого оточення співробітника (його друзів, партнерів по спілкуванню, відпочинку, інтересам). Воно дозволяє побачити особистість як би відбитої від інших. Адже тривале активне співробітництво, симпатія, дружба можливі тільки на основі подібних смаків, поглядів, переконань, способу життя. На жаль, спосіб спостереження вимагає значних витрат часу й сил, тому він використається тільки відносно постійного персоналу, що має більш-менш солідний стаж роботи у фірмі.

Крім того, треба пам'ятати, що спостереженням спеціально ніхто займатися не буде. Комерційна фірма - не філія контррозвідки. Тому справа знов-таки зводиться до опитування для виявлення думок одних співробітників про інші. І отут важливо мати на увазі, що джерелом найбільш достовірної інформації може бути лише така людина, що максимально об'єктивна у своїх оцінках, неупереджено ставиться до особистості кандидата, уміє розбиратися в людях і будувати свої висновки на основі перевіреного фактичного матеріалу. Як ми всі знаємо, що найчастіше глава фірми судить про своїх співробітників на основі думок фаворитів, у числі яких - родичі, що працюють у фірмі, друзі дитинства, коханки та інші, чиї судження досить далекі від реального положення речей.

Найбільш точні відомості про людину, притім у найкоротший термін, дає психологічне тестування. Однак верх наївності думати, що достовірний психологічний портрет свого співробіт-ника може одержати будь-який його начальник, якщо тільки вмовить відповісти на питання тих «жартівних псевдо тестів», які удосталь публікуються на сторінках популярних журналів. Про спеціальні тести, які застосовуються для науково обґрунтованого вивчення особистості, ми розповідали в попередніх розділах. Необхідно підкреслити, що правильно працювати з такими тестами можуть тільки професійні психологи.

Соціально-психологічний тренінг, що моделює конфліктні й стресові ситуації, що виникають у процесі спільної трудової діяльності, дає ще більше адекватної інформації про кандидата, чим тестування. Але й кваліфікація психолога, що здійснює такий тренінг, теж повинна бути на вищому рівні. До того ж, тренінг (особливо відеотренінг) коштує досить дорого, тому в більшості випадків керівники фірм можуть про нього тільки мріяти, та й то за умови, що розуміють його можливості.

Всі перераховані методи збору інформації переслідують одну мету: допомагають виявити ті особистісні якості, які сприяють забезпеченню безпеки фірми (у тому числі збереженню в таємниці її секретів) і ті, які цьому перешкоджають. При цьому варто ясно усвідомлювати, що ідеальних людей у природі не існує. Важливо не уподібнення ідеалу, а точне знання сильних і слабких сторін співробітників. Тоді стає можливим висування на самі відповідальні посади тих з них, у кого позитивні особистісні якості істотно переважають над негативними.

Необхідно знати, що в такий спосіб співробітник, що має обов'язки служби з справами комер-ційних таємниць, випробовує психологічний тиск, обумовлений специфікою цієї діяльності. Адже, збереження чого-небудь у таємниці суперечить потребі людини в спілкуванні за допомогою обміну інформацією. А взявши на себе зобов'язання дотримувати вимог режиму таємності, співробітник змушений діяти в рамках істотного обмеження своєї волі. Крім того, над ним щодня домокловим мечем висить погроза можливої втрати документа (або дискети), що містить комерційну таємницю. Психологічно слабкої людини подібний тиск може привести до стресів, нервовим зривам, розвитку перекручених похилостей й інших негативних наслідків.

Отже, які ж якості особистості співробітника не сприяють схоронності довірених йому секретів, хто зі співробітників у силу цього вимагає особливої уваги й підтримки з боку керівництва?

Спеціальні дослідження й практичний досвід показують, що до числа таких якостей відносяться наступні:

- емоційна нестійкість;
- низька самооцінка;
- розчарованість у своїх здатностях і можливостях;
- гостре невдоволення службовим або матеріальним становищем;
- набір таких якостей як облудність; недисциплінованість; неакуратність; безвідповідальність; боягузтво; заздрісність; крайній егоїзм;

схильність до пошуку радості або забуття в алкоголі, наркотиках, гострих відчуттях; хвастощі, прагнення здаватися значніше, ніж є, пускати "пил в очі"; невміння передбачати наслідки своїх учинків;

- завищена самооцінка свого "Я", своїх можливостей контролювати людей і ситуації й цілий ряд інших.

Відповідно, треба прагнути до того, щоб у людей, причетних до комерційних секретів фірми, зазначені якості або були відсутні, або не були розвинені занадто сильно. І все-таки , як уже сказане, головне - не те, які люди по своїй суті, а чим вони натхнені. Робіть їх своїми друзями, однодумцями, компаньйонами. Тоді вони навряд чи зрадять вас, тому що це стане рівноцінним зраді самим собі. Такий справжній зміст заклику до матеріального й морального стимулювання співробітників. Розглянемо деякі питання подібного стимулювання докладніше.

Моральне та матеріальне стимулювання співробітників

Найважливішими й визначальними в особистості є ті психічні якості, які регулюють і направляють її діяльність. Що ж спонукує людину до здійснення тих або інших учинків, що активізує його мислення й волю? Це потреби, що знаходять своє вираження в інтересах, прагненнях, бажаннях та інші.

Американський психолог А. Маслоу виділяє у людей п'ять груп основних потреб:

1. Фізіологічні;
2. У забезпеченні безпеки.
3. У спілкуванні й контактах з іншими людьми;
4. У суспільному визнанні своєї значимості, і придбанні більш високого соціального статусу;
5. У самореалізації.

Знаючи цей науково встановлений факт, грамотний керівник будь-якої фірми повинен так організовувати роботу, щоб кожен його співробітник одержував від роботи максимальне задоволення (повертаючись у цьому зв'язку до проблеми підбора відзначу, що найбільше задоволення людина одержує при заняттях тією діяльністю яка максимально відповідає його здатностям й інтересам).

Створюючи умови для задоволення співробітником його потреб у самореалізації здатностей і потенцій, у суспільному визнанні його значимості, можна в рамках фірми встановити сприятливий соціально-психологічний клімат, максимально знизити плинність кадрів, сформувати так

званий “фірмовий патріотизм”. У такій обстановці маловирегідна поява працівника, що намагається самоствердитися шляхом передачі конкурентам секретів, тобто шляхом зрадництва.

Виходячи зі сказаного, необхідно в роботі з персоналом керуватися наступними правилами:

- створити діючу систему матеріальних стимулів;
- забезпечити кожного співробітника довгостроковою роботою;
- ставитися до них як до самостійних індивідів;
- забезпечити участь у прибутках;
- створити можливості для просування по службі;
- забезпечити участь усього персоналу у виробленні рішень;
- створити гнучку систему, що не травмує, звільнень.

Крім того, американські фахівці в області протидії промисловому шпигунству рекомендують використати будь-яку можливість для пропаганди програм забезпечення економічної безпеки фірми; не періодично винагороджувати співробітників фірми за успіхи в цій роботі, а розробити комплекс дій стимулювання; додатково стимулювати участь співробітників фірми в реалізації програм забезпечення таємності.

Загальні напрямки забезпечення охорони секретів підприємства

Завдання першорядної важливості для підприємця - надійно перекрити канали витоку конфіденцій-ної інформації. Носіями її виступають люди, документи, вироби (зразки товарів або продукції), а також процеси. “Проколи” найчастіше трапляються саме в цих місцях. На них і зупинимося.

1) Люди. Не впевнений - не присвячуй

Дотримуйтеся “залізного” правила: коло осіб, причетних до комерційних таємниць Вашої фірми, повинен бути максимально звужений. Конфіденційною інформацією можуть розташовувати лише ті співробітники, які пов’язані з нею в силу своїх службових повноважень. Необхідно також установити строгий порядок допуску до переговорів із представниками інших фірм і до підписання різних документів - доручите це двом-трьом співробітникам, у надійності яких не сумніваєтеся.

2) Цінуй не “стукачів”, а інформаторів

Одержати відомості про надійність співробітників фірми можна з їхніх особистих справ, а також шляхом психологічного тестування, співбесід, негласного спостереження, конфіденційного опитування колег,

знайомих з ними по колишньому місцю роботи. Цим повинні з фахівці - психолог і досвідчений кадровик (корисним може виявитися досвід колишніх співробітників правоохоронних органів).

3) Виховай патріотів

Якщо у ваших підлеглих болить серце за справи фірми, можна не сумніватися, що з будь-якої ситуації вони вийдуть із честю. Бажано, щоб вони відчували потребу консультуватися з вами. Прищепити своїм співробітникам звичку ділитися прикростями й радостями, виховати з них дійсних патріотів фірми керівник може, грамотно застосовуючи систему матеріальних і моральних стимулів, дотримуючись психологічно вивіреної лінії поводження. Добре якщо над підходами до рішення цього завдання по вашому замовленню попрацюють фахівці.

4) Документи

У заставу серцевої дружби - пристойну зарплату поклади працівникові. Співробітник, зайнятий діловими паперами фірми, повинен бути вашою довіреною особою. Його обов'язок - організувати роботу з документами, що містять важливу інформацію, так, щоб виключити її витік на всіх етапах - від підготовки текстів до обліку й зберігання вступників і вихідних телеграм, листів, зразків і т.п. Витрати, пов'язані з організацією спеціального діловодства, як правило, швидко окупаються. Ідіть на них, не замислюючись, пам'ятаючи про те, що зарплата діловода - застава його відданості вашому бізнесу!

Якщо співробітник, що курирує вашу канцелярію, недостатньо досвідчений, нагадаєте йому про необхідність ведення спеціального журналу обліку вхідних, вихідних і внутрішніх документів, що містять конфіденційну інформацію. За допомогою такого журналу ви зможете періодично проводити інвентаризацію й вчасно знищити папери, що втратили для вас (але не для ваших конкурентів) усякий інтерес.

5) "Закодуй" поголовно всю інформацію.

Для запобігання несанкціонованого вторгнення в комп'ютерні бази даних кожний зі співробітників фірми повинен мати особистий код, що дозволяє користуватися лише тією інформацією, що має відношення до його службових обов'язків. Наявність подібних кодів - досить надійний захист від "мисливців" за вашими секретами. Не зневажайте нею.

6.) Контролюй канали інформаційних зв'язків.

Установите систему обмежень на використання відкритих каналів зв'язку для передачі конфіденційних відомостей. Під відкритими канала-

ми маються на увазі переговори з реальними й потенційними партнерами, владою, ділова переписка, надання документації компаньйонам і контрольним органам, реклама, спілкування із представниками преси, державних органів, громадських організацій.

7.) Засекречуй і контролюй.

Охороняйте від можливого підслуховування або сканування свої телефони, факси, комп'ютери, офіси, автомобілі, квартири. Використайте для цього апаратури, що засекречує, зв'язку (ЗАЗ), генератори перешкод, прилади для виявлення "жучків" і сканующих пристроїв, застосовуйте умовні кодові позначення. Який би технічно складною не здавалася вам "кругова оборона" проти електронного шпигунства, у нинішніх умовах саме складності в остаточному підсумку може й не вистачити. Тому радимо повністю покластися на поради відданих вам фахівців.

8.) Контроль і збереження продукції.

Організуйте надійний облік всіх товарів, промислових й експериментальних зразків, відомості про які не повинні стати надбанням ваших конкурентів. Охорона перерахованих вище виробів необхідна на всіх етапах їх "руху" усередині фірми (придбання або виготовлення, випробування або перевірка якості, транспортування, зберігання, експлуатація, ремонт і т.п.).

9.) Використовуйте технічні можливості.

Будь-яка фірма, будь-яке підприємство має різноманітні технічні засоби, призначені для прийому, передачі, обробки й зберігання інформації. Фізичні процеси, що відбуваються в таких пристроях при їхньому функціонуванні, створюють у навколишньому просторі побічні випромінювання, які можна виявляти (на досить значних відстанях (до декількох сотень метрів) і, отже, перехоплювати.

Фізичні явища, що лежать в основі випромінювань, мають різний характер, проте , витік інформації за рахунок побічних випромінювань відбувається по своїй "системі зв'язку", що складає з передавача (джерела випромінювань), середовища, у якій ці випромінювання поширюються, і приймача. Таку "систему зв'язку" прийнято називати технічним каналом витоку інформації.

Технічні канали витоку інформації діляться на:

- радіоканали (електромагнітні випромінювання радіодіапазону);
- електричні (напруги й струми в різних струмопровідних комунікаціях);

- акустичні (поширення звукових коливань у будь-якому звукопровідному матеріалі);
- оптичні (електромагнітні випромінювання у видимій, інфрачервоній й ультрафіолетовій частинах спектра).

Джерелами випромінювань у технічних каналах є різноманітні технічні засоби, особливо ті, у яких циркулює конфіденційна інформація. До їхнього числа відносяться:

- мережі електроживлення й лінії заземлення;
- автоматичні мережі телефонного зв'язку;
- системи факсимільного, телекодового й телеграфного зв'язку;
- засобу гучномовного зв'язку;
- засобу звуко- і відеозапису;
- системи звукопідсилення мови;
- електронно-обчислювальна техніка;
- електронні засоби оргтехніки.

Крім того, джерелом випромінювань у технічних каналах витоку інформації може бути голос людини. Середовищем поширення акустичних випромінювань у цьому випадку є повітря, а при закритих вікнах і дверях - повітря й різні звукопровідні комунікації. Якщо при цьому для перехоплен-ня використаються спеціальні мікрофони, то утвориться акустичний канал витоку інформації.

Важливо відзначити, що технічні засоби не тільки самі випромінюють у простір сигнали, що містять оброблювану ними інформацію, але й уловлюють за рахунок мікрофонів або антенних властивостей інші випромінювання (акустичні, електромагнітні), що існують у безпосередній близькості від них. Уловивши, вони перетворюють прийняті випромінювання в електричні сигнали й безконтрольно передають їх по своїх лініях зв'язку на значні відстані. Це ще більше підвищує небезпека витоку інформації. До числа технічних пристроїв, здатних утворювати електричні канали витоку відносяться телефони (особливо кнопкові), датчики охоронної й пожежної сигналізації, їхньої лінії, а також мережа електропроводки.

Заходи по створенню системи захисту об'єкта

Для створення системи захисту об'єкта від витоку інформації по технічних каналах необхідно здійснити ряд заходів. Насамперед , треба проаналізувати специфічні особливості розташування будинків,

приміщень у будинках, територію навколо них і підведені комунікації. Потім необхідно виділити ті приміщення, усередині яких циркулює конфіденційна інформація й урахувати використовувані в них технічні засоби. Далі варто здійснити такі технічні заходи:

1) перевірити використовувану техніку на відповідність величини побічних випромінювань припустимим рівням;

2) екранувати приміщення з технікою або цією технікою в приміщеннях;

3) перемонтувати окремі ланцюги, лінії, кабелі;

4) використати спеціальні пристрої й засоби пасивного й активного захисту.

Важливо підкреслити, що на кожен метод одержання інформації з технічних каналів її витоку існує метод протидії, часто не один, котрий може звести погрозу до мінімуму. При цьому успіх залежить від двох факторів: - від вашої компетентності в питаннях захисту інформації (або від компетентності тих осіб, яким ця справа доручена) і від наявності встаткування, необхідного для захисних заходів. Перший фактор важливіше другого, тому що сама вдосконалена апаратура залишиться мертвим капіталом у руках дилетанта.

У яких випадках доцільно проводити міри захисту від технічного проникнення? Насамперед , таку роботу необхідно здійснювати превентивно, не очікуючи поки "загримить грім". Роль спонукального мотиву можуть зіграти відомості про витік інформації, що обговорювалася в конкретному приміщенні вузькою групою осіб, або відпрацьовувалася на конкретних технічних засобах.

Поштовхом до дії можуть стати сліди, що свідчать про проникнення в приміщення вашої фірми сторонніх осіб, або якісь дивні явища, пов'язані з використовуваною технікою (наприклад, підозрілий шум у телефоні). Здійснюючи комплекс захисних мір, не прагніть забезпечити захист усього будинку. Головне - обмежити доступ у ті місця й до тієї техніки де зосереджена конфіденційна інформація (не забуваючи, звичайно, про можливості й методи дистанційного одержання її). Зокрема , використання якісних замків, засобів сигналізації, гарна звукоізоляція стін, дверей, стель і підлоги, звуковий захист вентиляційних каналів, отворів і труб, що проходять через ці приміщення, демонтаж зайвої проводки, а також застосування спеціальних пристроїв (генераторів шуму, апаратури

ЗАЗ й ін.) серйозно утруднять або зроблять безглуздими спроби впровадження спецтехніки.

Саме тому для розробки й реалізації заходів щодо захисту інформації від витоку по технічних каналах треба запрошувати кваліфікованих фахівців, або готовити власні кадри по відповідних програмах у відповідних навчальних центрах.

Для стислості вмовимося, що абревіатура «ТЗПІ» позначає Технічні Засоби Передачі Інформації.

Наукові розробки весь час ідуть вперед, тому ми надамо читачеві тільки загальні напрямки щодо захисту інформації від витоку по технічним каналам, декому вони будуть казатися застарілими, але вони мають основну перевагу, всі вони перевірені часом і дуже ефективні.

1.) Заземлення ТЗПІ. Однією з найважливіших умов захисту ТЗПІ є правильне заземлення цих пристроїв. На практиці найчастіше доводиться мати справа з радіальною системою заземлення, що має менше загальних ділянок для протікання сигнальних і живильних струмів у зворотному напрямку (від ТЗПІ до сторонніх спостерігачів).

Варто мати на увазі, що шина заземлення й заземлюючого контуру не повинна мати петель, а виконуватися у вигляді дерева з гілками, де опір контуру не перевищує один ом. Дана вимога задовольняється застосуванням у якості заземлених стрижнів з металу, що володіють високою електропровідністю, занурених у землю й з'єднаних з металевими конструкціями ТЗПІ. Найчастіше це вертикально вбиті в землю сталеві труби довжиною в 2-3 метра й діаметром 35-50-мм. Труби гарні тим, що дозволяють досягати вологих шарів землі, що володіють найбільшою провідністю й не підданих висиханню або промерзанню. Крім того, використання труб не зв'язано зі скільки-небудь значними грабарствами .

Опір заземлення визначається головним чином опором розтікання струму в землі. Його величину можна значно знизити за рахунок зменшення перехідного опору (між заземленим металом і ґрунтом), шляхом ретельного очищення поверхні труби від бруду й іржі, підсипанням у лунку по всій її висоті повареної солі й ущільненням грунту навколо кожної труби. Заземлені труби варто з'єднувати між собою шинами за допомогою зварювання. Перетин шин і магістралей заземлення заради досягнення механічної міцності й одержання надійної провідності рекомендується брати не менш 24х4 мм.

Магістралі заземлення поза будинком треба прокладати на глибині близько 1,5 метра, а усередині будинку - по стінах або спеціальних каналах, щоб можна було їх регулярно оглядати. З'єднують магістралі із заземленими трубами тільки за допомогою зварювання, а до ТЗПІ магістраль підключають болтовим з'єднанням в одній крапці. У випадку підключення до магістралі заземлення декількох ТЗПІ - з'єднувати їх з магістраллю треба паралельно (при послідовному з'єднанні відключення одного ТЗПІ може привести до відключення всіх інших). Для створення заземлення ТЗПІ не можна застосовувати уже існуючі природні заземлення: металеві конструкції будинків, що мають з'єднання із землею, прокладені в землі металеві труби, водогін, газову магістраль, металеві оболонки підземних кабелів та інше.

При розрахунку конкретних заземлюючих пристроїв необхідно використати спеціальні формули й таблиці. Ці дані ми будемо давати студентам на лекціях.

2.) Мережні фільтри. Виникнення наведень у мережах харчування ТЗПІ найчастіше пов'язане з тим, що вони підключені до загальних ліній харчування.

Тому мережні фільтри виконують дві функції в ланцюгах харчування ТЗПІ:

1) - захисту апаратури від зовнішніх імпульсних перешкод;

2) - захисту від наведень, створюваних самими апаратурами.

При цьому однофазна система розподілу електроенергії повинна здійснюватися трансформатором із заземленою середньою крапкою, трифазна - високовольтним понижуючим трансформатором.

При виборі фільтрів потрібно враховувати: номінальні значення струмів і напруг у ланцюгах харчування, а також припустимі значення спадання напруги на фільтрі при максимальному навантаженні; припустимі значення реактивної складової струму на основній частоті напруги харчування; необхідне загасання фільтра; механічні характеристики фільтра (розмір, маса, тип корпуса, спосіб установки); ступінь екранування фільтра від сторонніх полів.

Фільтри в ланцюгах харчування повинні мати досить різні конструкції, їхня маса коливається в межах від 0,5 кг до 90 кг, а обсяг від 0,8 див3 до 1,6 м3. Конструкція фільтра повинна забезпечувати істотне зниження ймовірності виникнення усередині корпуса побічного зв'язку між входом і виходом через магнітні, електричні або електромагнітні поля.

3.) Екранування приміщень. Для повного усунення наведень від ТЗПІ в приміщеннях, лінії яких виходять за межі контрольованої зони, треба не тільки придушити їх у проводах, що відходять від джерела, але й обмежити сферу дії електромагнітного поля, створюваного системою його внутрішніх електропроводок. Це завдання вирішується шляхом екранування.

Теоретично, з погляду вартості матеріалу й простоти виготовлення, переваги на стороні екранів з листової сталі. Однак застосування сітки значно спрощує питання вентиляції й висвітлення. Щоб вирішити питання про матеріал екрана, необхідно знати, у скільки разів потрібно послабити рівні випромінювання ТЗПІ. Найчастіше це між 10 й 30 разів. Таку ефективність забезпечує екран, виготовлений з одинарної мідної сітки з осередком 2,5 мм, або з тонколистової оцинкованої сталі товщиною 0,51 мм і більше.

Металеві аркуші (або полотнища сітки) повинні бути між собою електрично міцно з'єднані по всьому периметрі, що забезпечується електрозварюванням або пайкою. Двері приміщень також необхідно екранувати, із забезпеченням надійного електроконтакту з дверною рамою по всьому периметрі не рідше, ніж через 10-15 мм. Для цього застосовують пружинну гребінку з фосфористої бронзи, зміцнюючи її по всьому внутрішньому периметрі дверної рами. При наявності в приміщенні вікон їх затягують одним або двома шарами мідної сітки з осередком не більш ніж 2х2 мм, причому відстань між шарами сітки повинне бути не менш 50 мм. Обидва шари повинні мати гарний електроконтакт зі стінками приміщення за допомогою все тієї ж гребінки з фосфористої бронзи, або пайкою (якщо сітка незнімна).

Розміри екрануємого приміщення вибирають, виходячи з його призначення, наявності вільної площі й вартості робіт. Звичайно досить мати приміщення площею 6-8 кв. метрів при висоті 2,5-3 метри.

4.) Захист телефонів і факсів. Як усякий електронний пристрій, телефон і факс, а також їхньої лінії зв'язку випромінюють у відкритий простір високі рівні поля в діапазоні частот аж до 150 мгц.

Щоб повністю придушити всі види випромінювань від цих ТЗПІ, необхідно відфільтрувати випромінювання в проводах мікротелефону, у проводах відхідних від апарата, а також забезпечити достатню екраніровку внутрішньої схеми апарата. Те й інше можливо лише шляхом значної переробки конструкцій апаратів і зміни їхніх електричних

параметрів. Іншими словами, потрібно захистити ланцюг мікрофона, ланцюг дзвінка й двопровідну лінію телефонного зв'язку. Зрозуміло, що здійснити зазначені заходи здатні тільки фахівці з використанням відповідного встаткування й стандартних схем. Те ж саме ставиться й до проблеми захисту ліній зв'язку, що виходять за межі приміщень із апаратами.

Загалом кажучи, це дуже серйозна проблема, тому що подібні лінії практично завжди безконтрольні й до них можна підключати найрізноманітніші засоби знімання інформації. Отут два шляхи:

- По-перше, застосовують спеціальні проведення: (екранований біфіляр, тріфіляр, коаксильний кабель, екранований плоский кабель).
- По-друге, систематично перевіряють спеціальними апаратурами, є чи факт підключення засобів знімання інформації.

Виявлення наведених сигналів звичайно виробляється на границі контрольованої зони або на комутаційних пристроях у кросах або розподільних шафах. Потім або визначають конкретне місце підключення, або (якщо таке визначення неможливо) улаштовують шумовий захист.

Але найбільш ефективний спосіб захисту інформації, переданої по телефоні або факсу - це використання ЗАЗ (засекречуваної апаратури зв'язку). За рубежем дані пристрої називають скремблери. Один із кращих апаратів такого роду має наступні габарити: 26,5 х 16 х 5 см., маса 1,3 кг. Споживана потужність не більше 5 ватів. У країнах СНД (Росія, Україна) роблять ЗАЗ на рівні найвищих міжнародних вимог.

5.) Захист від убудованих й вузьконаправленних мікрофонів.

Мікрофони, як відомо, перетворять звук в електричний сигнал. У сукупності зі спеціальними підсилювачами й фільтрами вони можуть використатися як підслуховующий пристрій. Для цього створюється схована провідна лінія зв'язку, виявити яку можна лише фізичним пошуком або (що складніше) шляхом контрольних вимірів сигналів у всіх проводах, наявних у приміщенні. Методи радіоконтроля, ефективні для пошуку радіозакладок, тому у цьому випадку їх використання – не доцільне..

Крім перехоплення звукових коливань, спеціальні мікрофони-стетоскопи дуже добре сприймають звуки, що поширюються по будівельних конструкціях будинків. З їхньою допомогою здійснюють підслуховування через стіни, двері й вікна. Нарешті, існує ряд модифікацій вузьконаправленних мікрофонів, що сприймають і підсилює звуки, що йдуть тільки з одного напрямку, а всі інші звуки, послабляють при цьому. Такі мікрофо-

ни мають вигляд довгої трубки, батареї трубок або параболічної тарілки з конусом концентратора. Вони вловлюють звуки голосу на відстанях до одного кілометра!

Для захисту від вузьконаправленних мікрофонів можна рекомендувати наступні міри:

- всі переговори проводити в кімнатах, ізольованих від сусідніх приміщень, при закритих дверях, вікнах і кватирках, запнутих щільних шторах. Стіни також повинні бути ізольовані від сусідніх будинків;
- підлоги й стелі повинні бути ізольовані від небажаного сусідства у вигляді агентів з мікрофона-ми й іншою апаратурами прослуховування;
- не ведіть важливих розмов на вулиці, у скверах й інших відкритих просторах, незалежно від того, сидите ви або прогулюєтеся;
- у ресторані, іншому закритому приміщенні поза офісом якщо буде потреба обміну конфіденцій-ною інформацією, (для упередження слідкування за вами) змініть приміщення на інше, що перебуває під надійним контролем вашої служби безпеки (наприклад, окремий кабінет, замовлений раніше через надійного партнера або помічника);
- пом'ятайте, що спроби заглушати розмову звуками води, що ллється із крана (або з фонтана) малоефективні;
- якщо вам обов'язково потрібно щось повідомити або почути, а гарантій від підслуховування ні, говорите один одному пошепки прямо у вухо або пишіть повідомлення на листках, негайно після прочитання що спалюють.

6.) Захист від лазерних пристроїв, що підслухують. Лазери - це такі пристрої, у яких передача й одержання інформації здійснюється в оптичному діапазоні. Такі пристрої малогабаритні й економічні, тим більше, що як приймач нерідко використаються фотооб'єктиви з більшою фокусною відстанню, що дозволяє вести перехоплення сигналів з далеких відстаней. Принцип дії лазерного пристрою полягає в посилці зондувального променя в напрямку джерела звуку й прийомі цього променя після його відбиття від яких-небудь предметів.

Цими предметами, що вібрують під дією навколишніх звуків як своєрідні мембрани, можуть бути скла вікон, шаф, дзеркала, посуд і т.п. Своїми коливаннями вони модулюють лазерний промінь, прийнявши який через приймач можна досить просто відновити звуки мови. Розповсюджені нині лазерні пристрої дозволяють вільно підслухувати людську

мову крізь закриті вікна з подвійними рамами на відстанях від 100 до 250 метрів.

Найбільш простим й у той же час досить надійним способом захисту від лазерних пристроїв є створення перешкод для детектування за допомогою пьезоэлементів. Пьезоэлемент коливає скло з більшою амплітудою, чим голос людини, тому амплітуда вібрації скла виключає ведення прослуховування.

7.) Пошук радіозакладок. Радіозакладки займають провідне місце серед засобів технічного шпигунства. Вони бувають різних конструкцій, від найпростіших до дуже складних (мають дистанційне керування, систему нагромадження сигналів, систему передачі сигналів у стислому виді короткими серіями).

Для підвищення скритності роботи, потужність передавача радіозакладки робиться невеликою, але достатньої для перехоплення високочутливим приймачем з невеликої відстані. Робочу частоту для підвищення скритності нерідко вибирають поблизу несучої частоти потужної радіостанції.

Мікрофони роблять як убудованими, так і виносними. Вони бувають двох типів:

1.) - акустичними (тобто чутливими до голосів людей),

2.) - вібраційними (перетворюючими в електричні сигнали коливання, що виникають від людської мови в різноманітних жорстких конструкціях).

Радіозакладки найчастіше працюють на високих частотах (понад 300 кгц). Однак є й такі пристрої, які працюють у низькочастотному діапазоні (50-300 кгц). Як канал зв'язку - вони використають мережі електропроводки або телефонні лінії. Такі радіозакладки практично не випромінюють сигнали в навколишній простір, тобто мають підвищену скритність. Якщо їх вмонтувати в настільну лампу, розетку, трійник, будь-який електроприлад, що працює від мережі змінного струму, то вони, харчуючись від мережі, будуть довгий час передавати по ній інформацію в будь-яке місце будинку й навіть за його межі.

Для виявлення радіозакладок застосовують спеціальні вимірювальні приймачі, автоматично скануючі по діапазоні. З їхньою допомогою здійснюється пошук і фіксація робочих частот радіозакладок, а також визначається їхнє місцезнаходження. Дана процедура досить складна, вона

вимагає відповідних теоретичних знань, практичних навичок роботи з різноманітної, досить складними вимірювальними апаратурами.

Якщо радіозакладки виключені в момент пошуку й не випромінюють сигнали, по яких їх можна виявити радіоприймальними апаратурами, то для їхнього пошуку (а також для пошуку мікрофонів і пристроїв, що підслухують, (мінімагнитофонів) - застосовують спеціальну рентгенівську апаратуру й нелінійні детектори з убудованими генераторами мікрохвильових коливань низького рівня. Такі коливання проникають крізь стіни, стелі, підлога, меблі, портфелі, - у будь-яке місце, де може бути захована радіозакладка, мікрофон, магнітофон. Коли мікрохвилювий промінь стикається із транзистором, діодом або мікросхемою, промінь відбивається назад до пристрою. Таким чином, принцип дії в цьому випадку схожий на міношукач, що реагує на присутність металу.

У тих випадках, коли немає приладів для пошуку радіозакладок, або немає часу на пошук, можна користуватися генераторами перешкод для придушення приймачів. Вони досить прості, дуже надійні й повністю знімають інформацію з радіозакладок у широкому діапазоні частот.

8.) Захист персональних ЕОМ. Якщо персональна ЕОМ використається тільки одним користувачем, то важливо, по-перше, попередити несанкціонований доступ до комп'ютера інших осіб у той час, коли в ньому перебуває інформація і по-друге, забезпечити захист даних на зовнішніх носіях від розкрадання. Якщо ж персональна ЕОМ використається групою осіб, то крім зазначених моментів захисту, може виникнути необхідність запобігти несанкціонованому доступу цих користувачів до інформації один одного.

Крім того, у всіх випадках необхідно захищати інформацію від руйнування в результаті помилок програм й устаткування, зараження комп'ютерними вірусами. Однак проведення такої страховки - обов'язково для всіх без винятку користувачів ЕОМ і не треба робити з цього безпосередньої проблеми, захист інформації від конкурентів – це першочергова задача служби безпеки.

3.3. Загальні методи по забезпеченню власної інформаційної безпеки

Для забезпечення безпеки інформації використаються наступні методи:

1) засобу захисту обчислювальних ресурсів, що використають парольну ідентифікацію й обмежують доступ несанкціонованого користувача;

2) застосування різних шифрів, що не залежать від контексту інформації.

Нагадаємо, що в персональної ЕОМ як обчислювальні ресурси виступають оперативна пам'ять, процесор, убудовані накопичувачі на твердому або гнучкому магнітному дисках, клавіатура, дисплей, принтер, периферійні пристрої. Захист оперативної пам'яті й процесора передбачає контроль за появою в оперативній пам'яті так званих резидентних програм, захист системних даних, очищення залишків секретної інформації в не використаних областях пам'яті. Для цього досить мати у своєму розпорядженні програму перегляду оперативної пам'яті для контролю за складом резидентних програм й їхнім розташуванням.

Набагато важливіше захист убудованих накопичувачів. Існують кілька типів програмних засобів, здатних вирішувати це завдання, ми зупинимося на трьох:

- захист диска від запису й читання;
- контроль за звертаннями до диска;
- засобу видалення залишків секретної інформації.

Але самий надійний метод захисту, безумовно, шифрування, тому що в цьому випадку охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки дискети). Однак у ряді випадків використання шифрування важко або неможливо, тому необхідно використати обидва методи в сукупності. Більшість засобів захисти реалізуються у вигляді програм або пакетів програм, що розширюють можливості стандартних операційних систем, а також систем керування базами даних.

Ознаки того, що Вас можливо прослуховують, із досвіду США. Розглянемо деякі із них.

Попереджуючі ознаки схованого прослуховування або установки закладок

1.) Вашим конкурентам можуть бути відомі ваші професійні секрети або конфіденційні питання бізнесу.

Це найбільш загальний показник. Крадіжка конфіденційної інформації - є багатомільярдною ($) індустрією в Сполучених Штатах. Часто, про те, що відбувся витік інформації, Ви не знаєте й не догадаєтеся як це трапилося.

2.) Секретні наради й установлювані ціни, насправді менш секретні.

Конфіденційні наради й установлювані ціни є дуже популярними цілями для шпигунів, що діють проти корпорацій. Як Вам сподобається, якщо плани корпорації, що прийняла Ваші пропозиції по плануванню, стали широко відомими? Чи не будуть копії креслень ваших виробів корисні для ваших конкурентів?

3.) Схоже, що людям відомо про Вашу діяльність, коли цього не повинне було б бути.

4.) Ви звернули увагу на дивні звуки або зміни напруги на ваших телефонних лініях, необхідно, своєчасно прийняти протидії.

Загальні помилки вітчизняних бізнесменів

Як указують відкриті джерела, автори інших видавань, вітчизняні бізнесмени роблять декілька загальних помилок, а потім звертаються за допомогою в охоронні фірми з таких причин :

1. Проблема повернення засобів (не надходить плата за відвантажений товар, не надходить оплачений товар, не повертається в зазначений строк кредит);
2. Проблема особистої безпеки бізнесменів і членів їхніх родин у зв'язку з погрозами й вимаганням;
3. Розкрадання вантажів на транспорті;
4. Крадіжки особистого майна у квартирах, офісах, котеджах, заміських будовах; пограбування; викрадення автомобілів;
5. Викрадення комерційної інформації (крадіжка документів, їхнє копіювання, знімання інформації з комп'ютерів і факсів, прослуховування й запис телефонних повідомлень, розмов у приміщеннях, підкуп співробітників);
6. Крадіжки й пограбування в магазинах, складських і виробничих приміщеннях;

7. Псування майна й товарів. Підпали, тощо.

Багато з перерахованих злочинів можна було б запобігти, якби вчасно були вжиті заходи превентивного характеру, або звернулися що найменше до Інтернету. Чому ж вони не були здійснені? Розглянемо декілька загальних причин за викладенням інших авторів.

Причини помилок вітчизняних бізнесменів

1. Скаредність, (жадність). Занадто часто бізнесмени (і фірми в цілому) елементарно жалкують виділити кошти на охорону й охоронні заходи. Вони сподіваються на "либонь", на чудо, на випадок, на що завгодно, тільки не на те, що треба. Потім, коли доводиться витрачатися на ремонт, на пошук зниклого, на виплату данини рекетирам, на лікарів, на відшкодування збитків, наступає прозріння. Але це потім, коли пробуджується "міцний задній розум". Звідси справедливість висловлення, відповідно до якого "скупий платить двічі, а те й тричі".

2. Неуцтво. Бізнесмени не розуміють суті комплексних охоронних заходів і того факту, що забезпечити розробку й здійснення такого комплексу здатні лише професіонали. Їхня збиткова логіка така: "я був досить розумний, щоб сколотити капітал, мені вистачить розуму й для того, щоб передбачити будь-яку небезпеку". Іншими словами, друга причина - після жадібності - це неуцтво;

3. Нецивілізованість, тобто відсутність досвіду комерційної діяльності за правилами ринку, а не колгоспного базару. Звідси випливає побоювання звертатися до фахівців за консультаціями по тим питанням, у яких бізнесмен некомпетентний, невміння "планувати ризик", відсутність такої обов'язкової й важливої процедури, як збір конфіденційної інформації про партнерів, контрагентів і кредиторів. Суцільно й поруч доводиться бачити, як підприємець "залітає" через те, що повірив на слово, неправильно склав найважливіший договір, переоцінив свої аналітичні можливості, не вивчив ринкову кон'юнктуру, навіть не догадувався про те, що всі його "комерційні таємниці" прекрасно відомі конкурентам і так далі.

4. Неуважність. Технічне забезпечення безпеки виробничих, складських, конторських і житлових приміщень дуже часто залишає бажати багато кращого, або взагалі відсутній. Справа доходить до смішного: товар на мільйони рублів інший раз зберігається за звичайними дверима, зі звичайним дверним замком, а на вікнах немає ґрат!

Розглядаючи проблему особистої безпеки в широкому плані, треба визнати, що у своїй більшості бізнесмени легко уразливі. У безлічі фірм будь-якій сторонній людині не важко буде проникнути усередину офісу під якимсь приводом, увійти в будь-який кабінет, безшумно зарізати свою жертву (навіть кілька людей) і вийти, не залучаючи уваги. Не обов'язково різати, глушитель на стовбурі "Беретты М-71" (гарний пістолет вагою не більше 600 грам), або вітчизняний "ПСС" (вага з патронами 830 грам), дає можливість застрелити стільки людей, скільки патронів у магазині, тобто не менше 6-и, за 2 секунди. Ще простіше те, що: у товкотнечі вас можуть уколоти голкою, кінчик якої вмочили в препарат за назвою строфантин. Це отрута нервово-паралітичної дії, від якої ви вмрете за 30 секунд у результаті зупинки подиху.

Тому нормальний, розумний, завбачливий підприємець повинен думати про свою безпеку, пам'ятуючи, як він уразливий, і наскільки тендітне людське життя взагалі. Зрозуміло, все добре в - міру. Не можна впадати в жодну крайність: однаково погано, коли повна відсутність охорони й гранично-погано, коли зосередження думок і дій направлено тільки на власну безпеку.

Загальні рекомендації по забезпеченню Вашої життєдіяльності

Автори рекомендують проаналізувати і скористуватися наступними засадами, розробленими фахівцями "Шин Бет", служби державної безпеки Ізраїлю.

1. Сполучайте у своїй системі безпеки міри трьох видів:

- особисту охорону (охоронці й службові собаки),
- технічні засоби охорони (сигналізацію, бронежилети, замки, сейфи й ін.),
- правила поведінки для всіх членів родини й найманого персоналу;

2. Наявність однієї лише особистої охорони є недостатнім для гарантування 95% безпеки, (100% дає тільки Господь Бог). Завжди потрібно саме комплекс мір названих вище трьох видів;

3. Про ненадійність будь-якої міри безпеки варто судити по самому слабкому місцю в ній (як про міцність ланцюга судять по її слабкій ланці);

4. Всі використовувані міри безпеки повинні перебувати під постійним контролем глави фірми або її фахівця в області безпеки;

5. Вжиті заходи безпеки повинні сполучатися з умовами повсякденного життя підприємця, його родини, не перешкоджати роботі фірми;

6. Ефективність мір безпеки буде вище, якщо вони сплановані фахівцями в цій області, з урахуванням специфіки вашого бізнесу й місцевих умов;

7. У тих випадках, коли ймовірність здійснення замаху на вас різко зростає, необхідно не просто виконувати всі запобіжні заходи , а вводити якісно новий рівень безпеки (починаючи з інформаційного захисту й кінчаючи зміною місця проживання).Нарешті бізнесмен зрозумів, що проігнорувавши створення власної служби безпеки – це його велика помилка. Треба негайно приступити до створення такої служби безпеки.

Багатогранність сфери забезпечення безпеки фірми, включаючи захист її комерційних секретів, вимагає створення спеціальної служби для реалізації всіх захисних заходів.

Структура, чисельність і склад з безпеки фірми визначаються реальними фінансовими можливостями, масштабом комерційної діяльності, ступенем конфіденційності інформації. Залежно від цих факторів з безпеки може варіювати від двох-трьох чоловік, що працюють по сумісництву, до повномасштабної служби з розвитий структурою. Як це зробити автори детально розповідали в попередніх розділах книги.

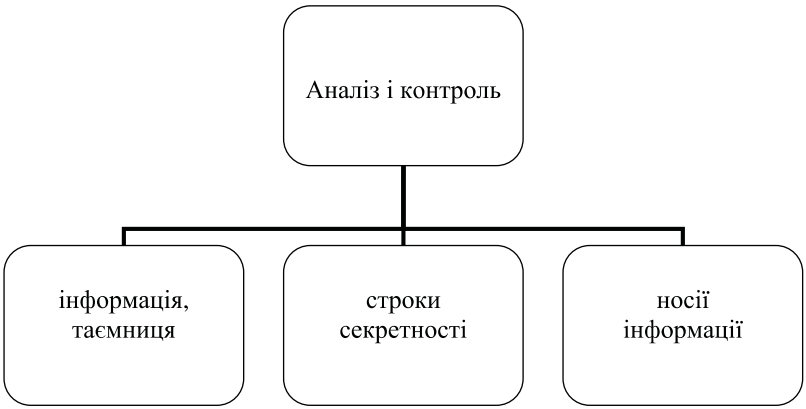
Висновки по безпеці витоку конфіденційної інформації

Таким чином, щоб відгородити себе від витоку конфіденційної інформації, треба:

- контролювати доступ співробітників фірми до закритої документації й до баз даних;
- періодично переглядати дані й визначати ступінь їхньої таємності, пам'ятаючи, що будь-яка інформація швидко "старіє";
- не зловживати найманням тимчасових співробітників, якщо вони по роду своєї роботи автоматично одержують доступ до конфіденційної інформації;
- обладнати звуконепроникні (екрановані) приміщення для обговорення важливих питань;
- регулярно обстежити такі приміщення, перевіряючи за допомогою спеціальних апаратур наявність у них що підслухують (сканующих) пристроїв;
- завести спеціальні конверти (папки), у яких конфіденційна інформація буде циркулювати усередині фірми;

- установити місця прийому відвідувачів, ніколи не залишати їх одних в офісі й інших приміщеннях фірми;
- не рідше одного разу в тиждень обстежити всі службові й підсобні приміщення фірми (включаючи коридори й туалети) для виявлення що підслухують і звукозаписних пристроїв;
- упорядкувати використання співробітниками множної й копіювальної техніки;
- установити апарат для знищення непотрібних документів (включаючи використаний копіювальний папір від друкарських машинок);
- неухильно дотримуватися правила: секретні документи знищуються особисто співробітником, відповідальним за безпеку фірми;
- використати для ведення службових записів тільки спеціальні зошити й блокноти, попередньо пронумерувавши їх;
- наприкінці робочого дня ховати ці зошити й блокноти в сейф або, у найгіршому разі, - у ящик стола, постачений надійним замком;
- установити персональну відповідальність співробітників за схоронність конфіденційної інформації із чіткою градацією мер дисциплінарного й матеріального впливу за її витік.

Кожен з незалежно від свого службового становища або ступеня споріднення з керівником фірми повинен володіти тільки тією інформацією, що йому необхідна для роботи.



Не забувайте про своїх конкурентів

Захищаючи власну інформацію, не забувайте накопичувати відомості про своїх конкурентів. Досьє на кожного із них може включати наступні розділи:

- ✸ організація й фінанси;
- ✸ комерційні можливості;
- ✸ плани й мети;
- ✸ збут;
- ✸ сильні й слабкі сторони.

Запам'ятайте: ситуацією володіє той, хто володіє інформацією.

Дотримуйтесь зальних застережень:

Дотримуючись наших порад, дійте кмітливо, головне - не перестарайтеся. Адже самий неприємний спогад, що залишається від фанатично виконаної молитви, - це розбите чоло. Пам'ятаючи про це, намагайтеся діяти так, щоб заходи щодо захисту інформації не йшли врозріз із загальною рекламною політикою, не заважали комерційній діяльності вашої фірми.

Розділ 4.

Робота з конфіденційними помічниками та конфіденційною інформацією

Програмна анотація

4.1. Організація роботи з конфіденційними помічниками,

– контакти з конфіденційними помічниками (КП),

– методика залучення до співпраці довірчих помічників (ДП),

– сихологічний стан самих працівникув СБ.

4.2. Захист, виявлення і перекриття каналів просочування конфіденційної інформації,

– організація захисту конфіденційного діловодства,

– загальні заходи з захисту конфіденційної інформації,

– заходи по внутрішній безпеці підприємства.

4.3. Службові розслідування.

4.4. Забезпечення кредитної політики банку, фірми, тощо.

– діяльність служби безпеки по розробці і реалізації кредитної політики банку

4.5. Внутрішне шахрайство на підприємстві,

– ознаки способів прихованого шахрайства.

4.6. Загальні проблеми діяльності підприємницької безпеки та шляхи іх вирішення.

4.1. Організація роботи з конфіденційними помічниками

Отримати актуальну, достовірну і повну інформацію про перебування справ на самому господарюючому суб'єктові і в навколишньому його середовищі неможливо без використання конфіденційних джерел інформації.

У даному розділі ми спробуємо детально розібратися із завданням залучення до довірчої співпраці інформаторів Служби безпеки.

Інформаційно-пошукова робота в недержавних структурах безпеки має на увазі, в першу чергу, роботу з так званим "людським чинником". Артур Шопенгауер із цього приводу якось відмітив: "Чим більше я дізнаюся про людей, тим більше люблю собак". "У розвідці немає покидьків, в розвідці є кадри" - вторить йому полковник Миколаі. Не сперечатимемося з класиками, а спробуємо за допомогою оперативної психології розібратися в тому, з ким нам завтра належить "йти в розвідку" і як, використовуючи спеціальні знання, можна з максимальною ефективністю виконати поставлене керівництвом - інформаційне завдання.

Інформатор (особа, що підтримує конфіденційні відносини із Службою безпеки) є головною фігурою в роботі підрозділів безпеки господарюючих суб'єктів. Їх придбання і цілеспрямоване використання складають основний зміст діяльності співробітників служби безпеки, (подальшому СБ) . Решта всіх засобів носить допоміжний характер.

База для залучення до співпраці вельми широка: ідеологічна близькість, користь, компрометуючі матеріали, незадоволеність керівництвом у зв'язку з тривалою затримкою просування по службі, утиск національної або людської гідності, заздрість, бажання помститися за уявні і справжні образи, авантюристські схильності, честолюбство і пихатість, самоту, нездатність завести сім'ю або коло близьких друзів, наявність одержимості або хобі.

Можна виділити три категорії інформаторів, вони можуть відноситися як до внутрішнього (контррозвідувальний підрозділ СБ), так і зовнішньому (розвідувальний підрозділ СБ) кругу забезпечення безпеки господарюючого суб'єкта:

1) довірчі помічники (**ДП**) - це ті, хто активно співробітничає з СБ;

2) довірчі контакти - виконуючі окремі завдання Служби безпеці. Вони зазвичай є об'єктами розробки для подальшого залучення їх як довірчі помічники;

3.) інші контакти - це ті, використання кого ведеться "навмання" і відбувається час від часу.

Підбір конфіденційних помічників, (інформаторів)

Отже, почнемо із самого початку. Оперативна психологія - не цілком наука. Це частково мистецтво, як і сама загальна психологія. Бо все, що має справу з людською свідомістю, не може претендувати на лаври строго наукової дисципліни: дуже невизначена матерія. Хоч би тому, що неможливо дотримати найважливіший критерій точної науки - повторюваність експерименту.

Підбір інформаторів є одним з найбільш делікатних моментів в роботі Служби безпеки. Помилка у виборі може обернутися не тільки особистою драмою людини, що виявила бажання співробітничати з СБ, але і провалом ретельно спланованого розвідувального або контррозвідува-льного заходу. При залученні до співпраці конкретної людини насамперед необхідно досліджувати його біографічні дані і скласти психологічний портрет.

На першому етапі вивчення кандидата або, як ми його називатимемо далі, об'єкту розробки (скорочено **ОР**), дуже корисний збір інформації із сторонніх джерел, наприклад, за місцем проживання і роботи (колишньої роботи) ОР (зашифрований опит сусідів і товаришів по службі про його поведінку, відношення до грошей, пристрасть до алкоголю і наркотиків, можливі відхилення в психічній і сексуальній поведінці).

Зібрана даним способом фактура хоч і є вельми поширеною формою отримання первинної інформації про об'єкт, в пряму використовується дуже рідко. Складений таким чином психологічний портрет може показатися достатньо повним, але повністю бути в цьому упевненим не можна, не враховуючи можливого свідомого спотворення ОР інформації про себе.

У розвідці і контррозвідці поспішні дії - недозволена розкіш, що часто закінчується «зірочкою на черговому обеліску». Щоб правильно оцінити поведінку об'єкту, необхідно з'ясувати - якими спонуками і якою інформацією, отриманою заздалегідь, він користується в своїх вчинках.

Для цього можна запропонувати наступну методику подальшої розробки об'єкту:

- встановлення і поглиблення безпосереднього особистого контакту з ОР. Його тестування;
- оцінка перспективності залучення ОР до співпраці;
- завершення контакту (у випадку, якщо по якихось причинах ОР опиниться непридатний для подальшого використання).

Встановлення і поглиблення безпосереднього особистого контакту з об'єктом. Його тестування

На даному етапі великий практичний інтерес представляють проектні методики дослідження особи об'єкту. Сенс їх полягає в тому, щоб "ненав'язливо" спонукати ОР до того, щоб він, обговорюючи, із його точки зору, безпечні теми, висловив би своє особисте відношення до змодельованої ситуації. В більшості випадків "Я" об'єкту мимоволі проектується на предмет і форму його розповіді і, розповідаючи про відвернуті речі, людина неминуче заносить в розповідь інформацію про себе самого.

В цілях виявлення відповідей, не відповідних дійсності, задаються спеціально підготовлені питання, по відповідях на яких можна судити про ступінь щирості того, що відповідає.

Алгоритм дослідження ОР за допомогою проектних методик дуже простий:

- в результаті оперативного управління бесідою загострити увагу досліджуваного на якій-небудь відвернутій темі;
- застосувавши стимулюючу комунікацію, уважно його вислухати;
- і, нарешті, розшифрувати отриману інформацію, ретельно проаналізувавши почуте.

Сильною стороною цієї методики є її комплексний підхід, тобто семантичний аналіз отриманих даних супроводжується зіставленням інформації, отриманої шляхом візуального контролю зовнішніх проявів емоційних переживань об'єкту. Саме поведінкові ситуації, незначні жести, окремі випадкові репліки ОР, відповідним чином оброблені і зіставлені, допомагають знайти необхідну транскрипцію сказаного і скласти цілісну картину.

"Не слухай, що говорять, дивися, що роблять", - говорили стародавні, і мали рацію. Вся сукупність дрібниць, спостережуваних в звичайній обстановці, повинна бути узагальнена, для того, щоб доповнити собою психологічний портрет кандидата по тих же параметрах, що і зібрана раніше інформація із сторонніх джерел: відношення до грошей і ма-

теріальної вигоди, до жінок і алкоголю, до хорошої кухні і подорожей, балакучість або стриманість, метушливість або скромність, швидкість або сповільненість рефлексів, імпульсна або холоднокровність, підозрілість або довірливість, проникливість або поверхневість.

Поглиблення контакту з ОР

У цій фазі розробки знайомства потрібно створювати приводи для повторних зустрічей, бо ніж більше побачень, тим сильніше вірогідність, що ті, що спілкуються сподобаються один одному. Потрібно, проте, прагнути до того, щоб ініціатива подальших зустрічей виходила від об'єкту.

Якщо об'єкт визнає, що позиція візаві відповідає очікуваною, знайомство заглиблюється, з'являються загальні теми для розмов, виникає спільність на основі індивідуальних переваг і емоційних співпереживань; у об'єкту з'являється активна симпатія до партнера.

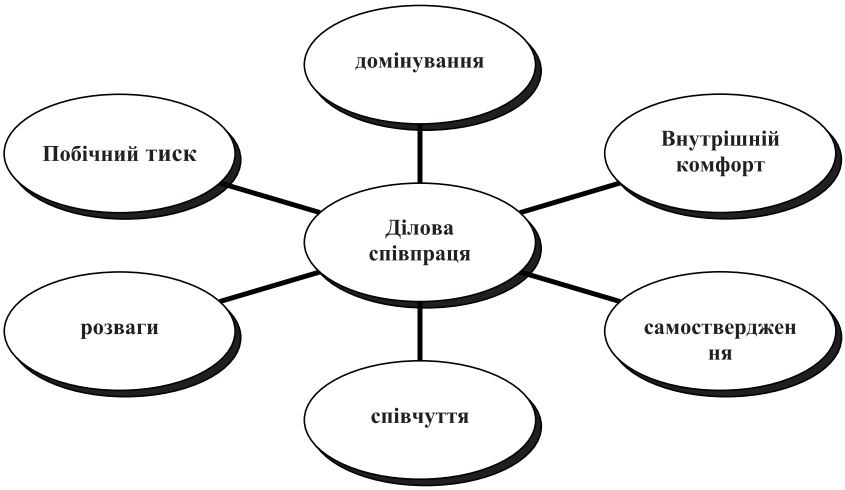
Основними спонуками до частішого спілкування тут можуть служити:

- потреба в домінуванні;
- потреба у внутрішньому комфорті (безпеці);
- потреба в самоствердженні;
- потреба в співчутті і розумінні;
- потреба в "розвагах";
- тиск з боку інших;
- бажання кооперації (ділової співпраці).

Точна конкретика мотивацій явно залежить від життєвих ситуацій людини і психологічних властивостей його особи.

Це спеціальна тема і потребує окремого, більш детального вивчення на семінарах.

Мотиви для поглибленного контакту об'єкта розробки



Оцінка перспективності залучення кандидата до співпраці

На перший погляд, здається, що не так вже важко скласти характеристику на людину, яка говорить більше, ніж потрібно. Проте не слід забувати, що об'єкт може видавати себе зовсім не за того, ким він є насправді. Виявлена спроба ввести в оману може означати дуже неприємні для працівника СБ - речі: від далекоглядності і досвіду ОР (об'єкт розробки), до підстави агента-двійника і спроби втягнути вас в чужу оперативну гру.

Основний упор при підборі ДП (довірчі помічники), слід зробити на урівноважених людей, що не прагнучих до дешевої популярності і не бравують своїми зв'язками із Службою безпеки. Довірчий помічник повинен уміти засвоювати велику кількість інформації в короткий час, при сильному збудженні і за наявності перешкод. Крім того, йому необхідний високий рівень оптимізму, здатність до інтенсивної діяльності, стійкість настрою і уміння чекати.

Найбільш важливими характеристиками професійної непридатності кандидата в ДП є наступні: багата уява, схильність придумувати події, невідповідні дійсності, або давати власне тлумачення оперативній обстановці, що склалася.

Дуже часто достовірність повідомлень ДП нівелюється рівнем довіри, що суб'єктивно склався, між ним і співробітником Служби безпеці, що займається ним. Завжди треба відокремлювати думку джерела з даного питання від фактів, що є у нього. Іноді буває так, що авторитет джерела підміняє собою його реальні можливості. До того ж, що не має спеціальної підготовки ДП може стати жертвою цілеспрямованої дезинформації.

У практиці роботи розвідки і контррозвідки для мінімізації суб'єктивності в оцінці отриманої оперативної інформації практикується її подвійна оцінка: оцінюється сама отримана інформація і джерело її отримання. Так, наприклад, якщо пацієнт психіатричної клініки розповідає про свій черговий політ на Місяць, зрозуміло, що адекватність джерела сумнівна, а сама інформація не витримує ніякої критики. Втім, в практиці бувають випадки, коли достовірна інформація поступає з ненадійного джерела, і навпаки.

Про операцію СБ , що проводиться, ДП повинен знати якомога менше. Найбільш оптимальним є варіант, коли довірчому помічникові не повідомляється про дійсну мету отримання інформації. При неможливості повного захування інформації про плановану акцію, в якій бере участь ДП, можливо легендування його участі (тобто повідомлення правдоподібної, але не відповідної дійсності інформації про мету і завдання даного заходу).

Можлива також видача декількох завдань, серед яких є одне, дійсно необхідне, а остальниє - абсолютно даремні для справи. В цьому випадку виконавець не може з ряду однотипних завдань виділити пріоритетну і, відповідно, не знає, що ж насправді цікавить Службу безпеки.

Розставання з довірчим помічником

Якщо розробка об'єкту стає, на думку співробітника СБ, безперспективна, подальші контакти з ним повинні бути припинені. Це може відбутися при різних обставинах: професійна непридатність об'єкту, об'єкт є "двійником", але можливості по його використанню в контргрі обмежені і, нарешті, при консервації контакту для можливого подальшого використання.

Методика залучення до співпраці ДП

Методика залучення до співпраці багатообразна, і не варто захоплюватися, набуваючи інформаторів тільки за гроші або шантажуючи їх зібраним "компроматом".

Матеріальне стимулювання, звичайно, повинне мати місце, але інформатор, що працює тільки за гроші, - ненадійний, оскільки легко може стати "двійником", надаючи "додаткові" послуги тому, хто заплатить більше, ніж ви.

У випадку, якщо отримання інформації неможливе без відвертої матеріальної основи, то психологічно дуже важливо - відразу дати гроші і вирішити їх витрачання. Не можна купувати людину теоретично.

"Нашій" людині необхідно не тільки побачити гроші живцем, але і помацати, понюхати і прикинути, як їх можна витратити. "Нашій" людині набагато простіше розлучитися з найкрупнішою, але невідчутною сумою, чим з найменшою, але утримуваною - в своїх руках.

Ще одне просте, але, на жаль, не завжди чітко усвідомлюване правило - не варто грубо сунути людині гроші, навіть якщо він сильно їх потребує. Матеріальний аспект співпраці може розшифровуватися вельми неоднозначно: додатковий заробіток, комерція, надання разової послуги для придбання крупної речі, оплата медичних витрат, пов'язаних з важкою хворобою, безкоштовний вояж за межу, фінансування підприємницької діяльності і таке інше…

У плані залучення до співпраці за допомогою компрометуючих матеріалів важливо пам'ятати, що людина з сильною нервовою системою, яку зламали на "компроматі" як жертва насильства, підсвідомо жадатиме реваншу і що цілком можливо, одного разу може спробувати його узяти. Людина із слабкою нервовою системою може видати на такий "жорсткий" вербовочний вихід неадекватну реакцію.

У практиці розвідувальної і контррозвідувальної діяльності мають місце факти підстави опонентами помилкового джерела через ретельно змодельований на нього "компромат".

По-перше, при використанні опонентами "двійника", йде "засвічення" напряму вашого разведінтереса відносно різних об'єктів і суб'єктів.

По-друге, передавши декілька щодо достовірних повідомлень, таке джерело починає гнати відверту "дезінформацію", яку сторона, що використовує його, зазвичай заковтує "за чисту правду". "Джерелами дезинформації треба уміти дорожити" - любив промовляти Аллен Даллес, і в даному випадку, ми думаємо, варто повірити старому асу на слово.

Як вже мовилося вище, не варто надавати очолюючому змісту матеріальному стимулюванню, але показувати свою увагу не великими по-

дарунками або урочистим обідом на честь знаменних для цієї людини дат і подій просто необхідно.

Більшість людей, перш за все, дорожать увагою до своєї персони, а не ціною отриманого подарунка. Ідеальний інформатор - той, хто працює на "ідейних" мотивах, до речі кажучи, ці мотиви можуть бути найрізноманітнішими і іноді зводяться до природної схильності людини до балакучості, інтриг або доносительства. Але найчастіше зустрічаються люди, що йдуть на співпрацю від відчуття самоти, від бажання усвідомити свою потрібність, хоч би кому-небудь, навіть таким "специфічним" способом. Для такої людини оперативник, що займається ним, зазвичай стає найближчою людиною.

При залученні до співпраці необхідно діяти дуже делікатно, ненав'язливо, не лізти, що називається, в душу з розпитуваннями, шукати загальні точки зіткнення і загальні інтереси, уважно придивлятися до об'єкту розробки, виявляти його життєві цінності і пріоритети, а, головне, слабкі і уразливі місця, застосовуючи які, можна його ефективно використовувати.

Кожної людини, в першу чергу, більше всього хвилюють його власні проблеми, а в повсякденному житті кожна людина страждає більше всього від того, що його ніхто не слухає. Найбільша проблема для більшості людей - знайти собі тактовного і уважного слухача.

Головне в мистецтві залучення до співпраці - це уміння уважно, не перебиваючи, слухати свого співбесідника, і якщо у об'єкта є бажання, коректно і з повагою обговорити тему, що хвилює його.

Молодий працівник служби безпеки повинен запам'ятати, що саме у цьому і полягає головна формула успішної роботи з джерелами інформації.

Якщо інформатор в даний момент повідомляє вам відомості, що не представляють для вас інтересу, його все одно необхідно вислухати з виразом крайній зацікавленості на обличчі і сердечно поблагодаріть після зустрічі за отримані цінні відомості. Проте слід пам'ятати, що невміння тактовне вивести співбесідника з тривалого безрезультатного монологу - показник низької професійної кваліфікації самого оперативника.

Інформаторів потрібно берегти і фізично, і психологічно, і емоційно. Але ні за яких обставин ДП не повинен ставати товаришем, оскільки в цьому випадку виникає своєрідна емоційна залежність. І той,

хто порушує це "золоте" правило, розплачується за прейскурантом в повному об'ємі. Особливо, якщо в ролі довірчого помічника виступає жінка.

При роботі з "слабкою" статтю слід враховувати ще одну особливість - жінки здатні на абсолютно нелогічний, дурний, нез'ясовний вчинок, продиктований виключно якими-небудь сьогохвилинними емоціями, і що найнеприємніше, ніхто не може передбачити, коли саме ці емоції виникнуть, - навіть сама жінка.

Психологічні особливості співпраці з ДП

Тепер давайте поговоримо про речі, які вам обов'язково доведеться використовувати в практиці інформаційно-пошукової роботи, це так звані людські комплекси. Якщо говорити строгою медичною мовою, то,те що в побуті маємо на увазі під людским комплексом, насправді - невроз.

А неврози є майже у всех, запам'ятатайте, не має абсолютно здорових людей, навчіться використовувати різні комплекси людей з користю для роботи.

Всі комплекси, які є у людини, формуються до 5-річного віку, коли дитина росте як особа. У нас прийнято виховувати, головним чином, за принципом: « забороняти і умовляти». "Якщо ти зараз робитимеш це, то я зроблю для тебе - те", "Якщо не слухатимешся мене, то я тебе любити не буду". Дитина зростає з підсвідомим відчуттям, що любити можна тільки "за щось". І людина все життя підсвідомо пригнічує свою особу, прагнучи стати "таким", щоб його любили, носить маску. Але рано чи пізно це може привести до невротичного комплексу, антисоціальної поведінки, озлобленості або депресії: Це загальні компенсаторні реакції організму, щоб "утриматися на плаву".

Комплекс неповноцінності, наприклад, виникає, по Адлеру, у будь-якої дитини, оскільки той малий, «неуміка», слабкий і повністю залежить від своїх батьків. Під зовнішньою розкутістю, підкресленою сексуальністю дуже часто ховається компенсація внутрішньої скутості, зажатості пригніченого жіночого єства.

Повна відсутність комплексів - це теж комплекс, тільки складніший "комплекс повноцінності". Те, що раніше називали манією величі. Людина, яка демонструє, що він - найкращий, розумніший, сильніший, красивіший, удачливіший і т.д., як правило, - компенсує таким чином своє глибинне відчуття неповноцінності. Той, хто дійсно упевнений в собі, не потребує того, щоб щохвилини доводити це. Серед різних наук по вивченню мозга і психики людини – нейропсихология займає провідне місце і

дуже добре цю тему розкриває відомий учений, доктор психологічних наук, доктор педагогічник наук, профессор,академик Макаров Р.Н., слід наголосити, що один із авторов данного виданная е його учнем. Більш детально ця тема буде розкрита на практичных семинарах.

Ситуація, коли людина знаходиться у контакті з працівником СБ, сама по собі невротична. До того ж невротик автоматично виробляє в собі невротичне відношення до всіх значущих для нього подій і осіб. При цьому, ДП починає розповідати оперативникові про себе ВСЕ підряд без приховування, в цьому і полягає основна схожість оперативника і психоаналітика. Такого роду відносини стають дуже значущі. Набуваючи щирого слухача, ДП набуває ще один невроз. Ризик тут, до речі, не так вже і великий, збільшення до багатьом неврозам ще одного вже ні на що істотно не впливає. Особливо це характерно для жінок.

Існують три типи прихильності:

1 - безопасностні,

2- що уникають усього, («избегатели»),

3- і тривожні (від любих подій).

Людина з безопасностним типом прихильності навіть в найгостріших ситуаціях не ускладнена внутрішніми проблемами і сумлінням. Він не позбавлений дару переживати, він швидше в подиві подумає про те: той, хто перестав з ним спілкуватися – «з'їхав зглузду», чим божеволіє сам.

Тип прихильності формується в ранньому дитинстві і залежить від того, як мати відносилася до своєї дитини - чи бігла до нього по першому заклику (безпечний тип), чи жорстко виховувала її, (дитина зростає "избегателем",уникає),або залишала дитину в невпевненості в материнському відчутті і чуйності (тривожний тип).

Люди з тривожним типом прихильності не впевнені в собі. Для них мірило власних можливостей і перспектив - не достоїнства їх особи, а відношення до них людей, що оточують їх.

За американськими даними у світі, тривожних людей - 25%, "избегателей", уникающих - 19%, а останні це безопасностні. Але це їх статистика. У наший країні людей з тривожним типом значно більше, що і дає працівникам СБ - великі оперативні можливості.

Про психологічний стан самих співробітників Служби безпеки

В наші дні уявлення про цю професію у широкого громадянства дуже часто формується по детективних романах і пригодницьких фільмах.

На жаль, більшість з них дає спотворену картину цієї важкої і невдячної роботи. Якщо судити по більшості творів, то співробітник підрозділів безпеки - це "квадратний" улюбленець жінок і завсідник ресторанів, що чудово володіє секретними прийомами єдиноборства, стріляє без промаху з будь-якого положення і здатний поодинці вирішувати будь-які завдання, лежачі за гранню неможливого.

Насправді, немає нічого дальшого від реальності. У повсякденному житті все зовсім не так. Не уміють колоти пляшки об власну голову і голови опонентів, а здатність аналізувати поточну оперативну обстановку і передбачати подальший хід розвитку подій - ось головне достоїнство людей Служби без пеки.

Хороший оперативник вже сьогодні повинен прогнозувати те, що його начальники зажадають від нього завтра. Це дуже важливо, оскільки завжди існує розрив тим часом, що може показатися корисним "в полі", і тим, що вважає важливим керівництво.

Для того, щоб якісно оцінити оперативну обстановку, що склалася, хаос життєвих подій і конфліктів, працівник СБ повинен знайти безпристрасну форму математичного завдання: дані початкової ситуації, подальші її зміні, відомі і невідомі величини, погодившись з якими доведеться діяти, засоби, що надаються в розпорядження, і нарешті, цілі операції.

Розумний і упевнений в собі оперативник не ганяється за інформаторами, як за жінкою, люди самі розкривають йому свої найпотаємніші таємниці.

Можна запропонувати наступну методологію аналізу, що складається з трьох етапів:

- перевірка своїх дій перед початком операції,
- під час дій,
- після закінчення дій.

Аналіз, передуючий будь-якому оперативному заходу, виключно важливий, оскільки готує вас до майбутніх дій, проте він ніколи не буває математично точним, оскільки ми маємо справу з лише вірогідністю події, тобто тим, що ще не відбулося, і невідомо, чи відбудеться це все так, як ми прогнозуємо. Аналіз під час дії украй необхідний, щоб не зробити помилкового кроку, проте він не такий глибокий, - немає часу на довгі роздуми. Аналіз після дії, навпаки, докладний і грунтовний, проте можливості щось

змінити вже немає. Кожен з цих способів по-своєму недосконалий, але всі вони спільно утворюють відмінний апарат.

Хороший працівник СБ повинен бути сильним не тільки фізично, але і морально. Якщо людина фізично здорова, це допомагає йому долати фізичні навантаження, більш того, дає можливість підходити до складних проблем, оцінюючи їх з граничною ясністю, незалежно від того - чи вирішувані вони чи ні.

Працівник структур безпеки набагато більш уразливий психологічно, ніж представник будь-якої іншої професії, адже робота примушує його жити в постійній напрузі. Для підтвердження цього твердження пошлемось на результати досліджень англійських психологів. Вони розробили шкалу частоти виникнення стресових ситуацій в професійній діяльності працівників. Виходячи з десятибальної оцінки, частота стресового стану в процентах:

- у шахтарів - 8,3,
- співробітників державних і недержавних структур правопорядку - 7,7,
- журналістів і льотчиків - 7,5,
- водіїв таксі - 6,8,
- вчителів - 6,2,
- продавців - 5,7,
- дипломатів і селян - 4,8,
- працівників банків і програмістів - 3,7,
- у працівників музеїв, що служать -2,8,
- у бібліотекарів - 2,0.

Це ще раз підтверджує, що потреба в знятті стресу є. Частий стрес, що виникає в процесі виконання роботи, багато хто намагається заглушити спиртним. Одних пригноблює відчуття провини, у інших складні відносини з жінками, у третіх в крові просто грає адреналін. Щоб якось розслабитися, просто необхідно мати якусь віддушину (хобі або захоплення чимось). Це дає можливість звільнитися, відпочити від нервової вимотуючої роботи. Коли людина розслабляється, розум його стає спокійнішим, думка - ясніше.

Уміння відключатися в будь-якій обстановці відрізняє професіонала від дилетанта. Працівник СБ повинен навчитися витрачати свою сіру речовину мозгу тільки тоді, коли це дійсно необхідно. У решту часу він повинен знаходитися в стані спокою. Інакше він не витримає такого життя й

одного тижденя. І якщо в художній літературі герої детективних романів не випробовують особливих психологічних проблем, то в реальному житті такі проблеми у працівників СБ стоять дуже гостро.

4.2. Захист, виявлення і перекриття каналів просочування конфіденційної інформації

Можна дати кілька загальних зауважень щодо створення системи захисту підприємства.

По-перше, фізична захищеність організації має розглядатися у тісній взаємодії з інформаційною. Однак ототожнювати їх не слід, адже заволодіти таємницями компанії сьогодні можна і не проникаючи в приміщення за міцними стінами. Досить потрапити в інформаційну систему, щоб отримати потрібні дані, вивести з ладу елементи корпоративної мережі або заблокувати доступ до інформаційних ресурсів.

По-друге, захист "всього й від усіх" не є раціональним і навряд чи принесе очікувані результати. Слід чітко визначити, яку інформацію потрібно оберігати в першу чергу й від кого. Для цього проводять аналіз можливих шляхів реалізації навмисних і випадкових атак, розробляють модель потенційного порушника, яка враховує його кваліфікацію, наявні засоби для здійснення атак, час дії, та прогнозують потенційні збитки.

По-третє, у середовищі, де людський фактор становить чи не найбільшу загрозу, особливо актуальним стає метод "батога і пряника". Йдеться про те, що організаційні та адміністративні заходи варто поєднувати з соціально-психологічними. Перші передбачають створення необхідної правової бази шляхом розробки організаційно-розпорядчих документів, на яких будується діяльність служб безпеки й відділів захисту інформації. Заходи ж соціально-психологічного характеру складаються з двох основних напрямів: правильного підбору кадрів і застосування матеріальних та моральних стимулів. За даними західних фахівців, від правильного підбору та стимулювання персоналу щонайменше на вісімдесят відсотків залежить збереження корпоративних таємниць. Одними з першочергових завдань досвідченого керівника вважають створення сприятливого соціально-психологічного клімату всередині організації, зниження плинності кадрів, формування "фірмового патріотизму". Не варто нехтувати впровадженням справедливої системи матеріальних винагород, ство-

ренням можливостей для професійного росту та для участі персоналу в прийнятті рішень. Тільки отримуючи максимальне задоволення від своєї роботи, працівник здатен виконувати свої обов'язки найбільш плідно.

Інформаційна безпека є однією із ключових засад добробуту бізнесу. Ефективна система захисту дає змогу уникнути прямих і непрямих збитків, зберегти довіру до компанії і навіть підвищити її прибутковість. Натомість не зупинені вчасно удари по інформаційних ресурсах знесилюють організацію, як задавнене захворювання виснажує людський організм. До речі, лікарі, як відомо, наголошують, що хворобі легше запобігти, ніж її лікувати.

Створення надійного механізму захисту комерційної таємниці вимагає проведення добре продуманих заходів. План їх здійснення повинен переслідувати **три мети**:

1 - запобігати крадіжці;

2 - дати всім зрозуміти, що для вас комерційна таємниця дуже важлива і що ви докладете всі зусилля для захисту останньої і покарання осіб, що розголошують або намагаються розголосити її;

3 - добитися, щоб ця програма якомога більше відповідала названим цілям. Приділивши достатньо часу розробці програми, і визначивши джерело фінансування її проведення, вирішите питання про призначення кого-небудь відповідальним за її постійне виконання і своєчасний перегляд.

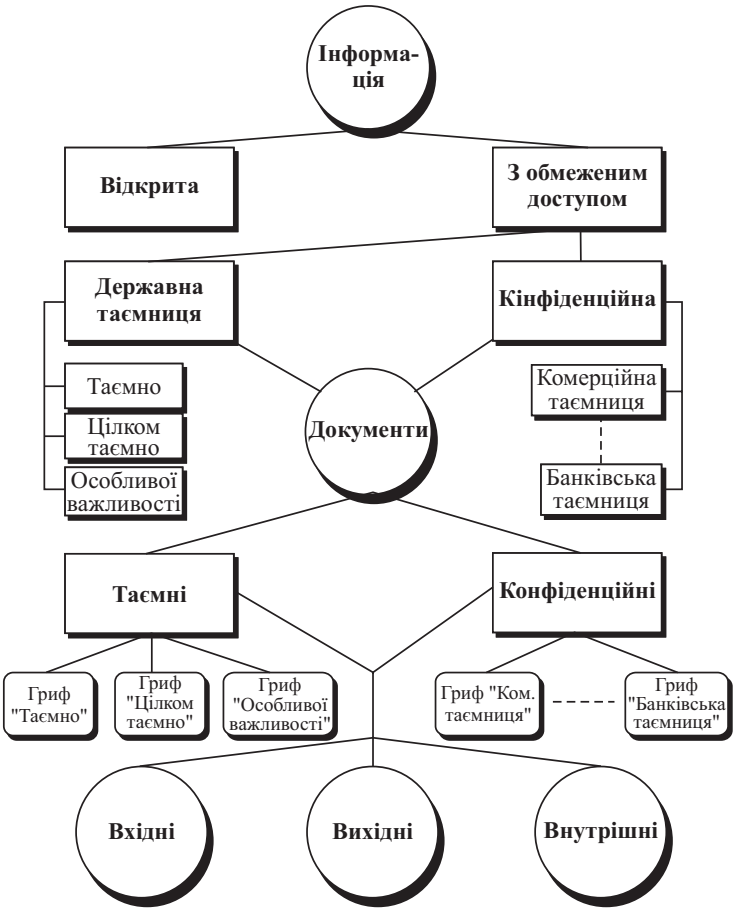
Цей працівник оцінюватиме ефективність програми і покращуватиме її час від часу. Організація ефективного захисту комерційної таємниці підприємства багато в чому залежить від правильного встановлення круга носіїв інформації. Аналіз в цій області дозволяє виділити чотири види носія інформації залежно від їх функціонального призначення, зокрема: документ, людина, виріб (предмет, матеріал) і процес.

Тому одному з першочергових завдань, які встають перед підприємством при організації захисту своєї комерційної таємниці, є розробка відповідних нормативних документів, що регламентують діяльність всіх ланок підприємства в цьому напрямі. Якщо звернутися до світової практики з даного питання, то мова, по суті справи, йде або про необхідність внесення відповідних доповнень в документи, що вже є на підприємстві, такі як Статут, Колективний договір і ін., або про підготовку самостійних внутрішніх інструкцій і рекомендацій.

Ці питання потребують детального розгляду, а тому будуть розглянуті в окремих лекціях та на практичних заняттях (семінарах).

Організація захисту конфіденційного діловодства

Правильна організація конфіденційного діловодства у фірмі є складовою частиною комплексного забезпечення безпеки інформації й має важливе значення в досягненні мети її захисту. Як відомо, фахівці, що займаються в області інформаційної безпеки, затверджують, що порядку 80% конфіденційної інформації перебуває в документах діловодства. Тому питання конфіденційного документообігу у фірмі безсумнівно відіграють



Мал.1. Види інформації й документів

важливу роль у досягненні нею економічних успіхів. У даній статті дані деякі рекомендації, що дозволяють упорядкувати роботу у фірмі з конфіденційними документами.

Всю інформацію у фірмі (організації) можна розділити на **дві великі групи**:

1) відкрита інформація;

2) з обмеженим доступом.

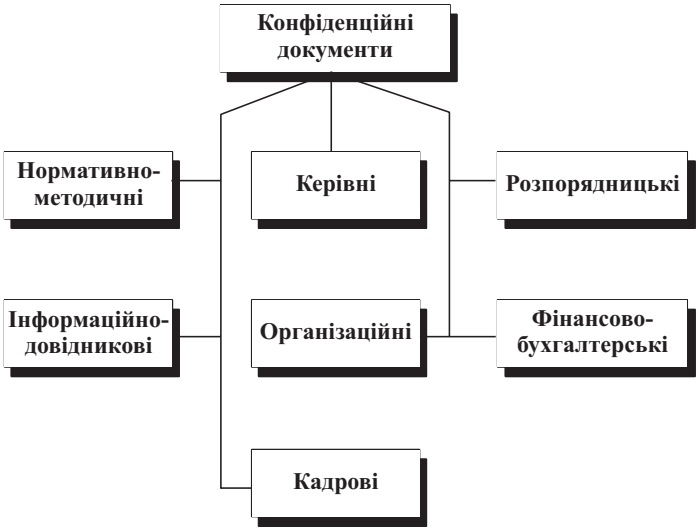
У свою чергу інформація з обмеженим доступом (Мал.1.) може бути:

- державною таємницею;
- конфіденційною інформацією.

А, отже, і документи, що містять ту або іншу інформацію підрозділяються на секретні й конфіденційні. Причому, секретні документи можуть бути із грифом "Секретно", "Абсолютно секретно", "Особливої важливості". Конфіденційні документи відповідно із грифами "Комерційна таємниця", "Банківська таємниця" і т.д. У цей час видів конфіденційної інформації (а, отже, і можливих секретних документів) налічується більше 30. Що в цілому не створює сприятливої атмосфери в змісті забезпечення їхньої безпеки. Із цієї причини кількість видів конфіденційної інформації в перспективі, треба думати, зменшиться. Кожен вид конфіденційних документів має реквізити.

По своїй природі (Мал. 2.) **конфіденційні документи бувають**:

- нормативно-методичні (НМД);
- керівні (РД);
- розпорядницькі (РПД);
- інформаційно-довідкові (ІСД);
- організаційні (ОД);
- фінансово-бухгалтерські (ФБД);
- кадрові (по особовому складі) КД.



Мал.2. Види конфіденційних документів

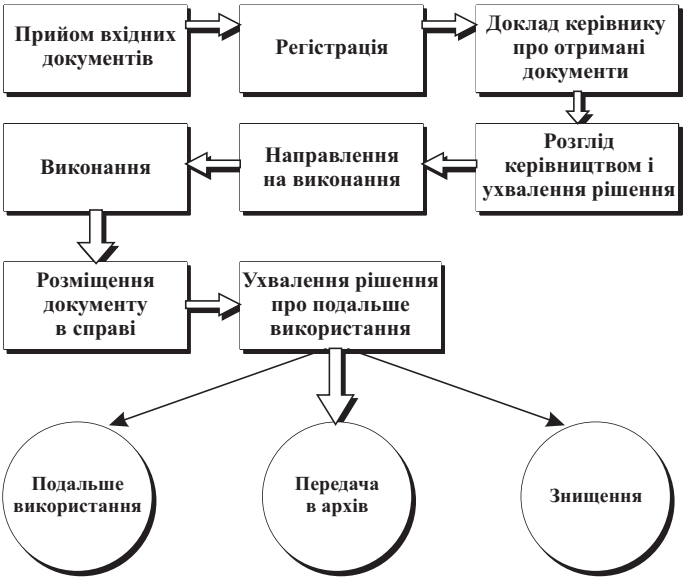
Правила оформлення реквізитів регламентована ДСТ "Уніфікована система організаційно-розпорядницької документації. Вимоги до оформлення документів". Конфіденційні документи, що містять комерційну таємницю, повинні мати гриф обмеження доступу до документа. Він розташовується в правому верхньому куті, наприклад: комерційна таємниця (або скорочено КТ). Доповнюється гриф номером екземпляра, наприклад, экз. №1.

Конфіденційні документи повинні оброблятися в конфіденційному діловодстві фірми, або в загальному діловодстві, спеціально призначеним посадовою особою, відповідальним за конфіденційні документи. Конфіденційні документи повинні зберігатися в окремому приміщенні в що замикають й опечатують шкафах, що. Допускається зберігання конфіденційних документів у загальному діловодстві. Але обов'язково вони повинні перебувати окремо від інших справ діловодства.

Залежно від призначення **конфіденційні документи підрозділяються на**:

- вхідні;
- вихідні;
- внутрішні.

Прийом вхідних конфіденційних документів (мал. 3) здійснюється співробітником конфіденційного діловодства.



Мал. 3. Порядок роботи із вхідними конфіденційними документами

При цьому перевіряється:

- кількість аркушів;
- кількість екземплярів;
- наявність додатків (якщо вони зазначені в супровідному листі).

У випадку відсутності в пакеті (конверті) деяких перерахованих документів - складається акт в 2-х екземплярах. Один екземпляр акту відправляється на адресу відправника.

Реєстрація конфіденційних документів виробляється в журналах реєстрації (мал. 4), або на картках.

№ п/п	Дата реєстрації документу	Дата і номер документу	Звідки поступив	Короткий зміст (найменування)	Кількість листів		К-сть екземплярів	Виконавець	Примітка
					Документу	Додатку			

Мал. 4. Журнал реєстрації вхідних конфіденційних документів

На кожному зареєстрованому документі повинен проставлятися штамп, у якому вказується:

- найменування;
- реєстраційний номер;
- дата надходження.

Після реєстрації документи передаються керівництву фірми для ухвалення рішення. Керівник після розгляду документа визначає виконавця й дає вказівки по виконанню документа. Ці вказівки оформляються на самому документі у вигляді резолюції.

З резолюцією керівника конфіденційний документ передається виконавцеві під розписку в журналі реєстрації вхідних конфіденційних документів (мал. 4).

По завершенні роботи над документом на ньому проставляється оцінка про його виконання й напрямок у справу. Після чого документ співробітником конфіденційного діловодства підшивається в справу.

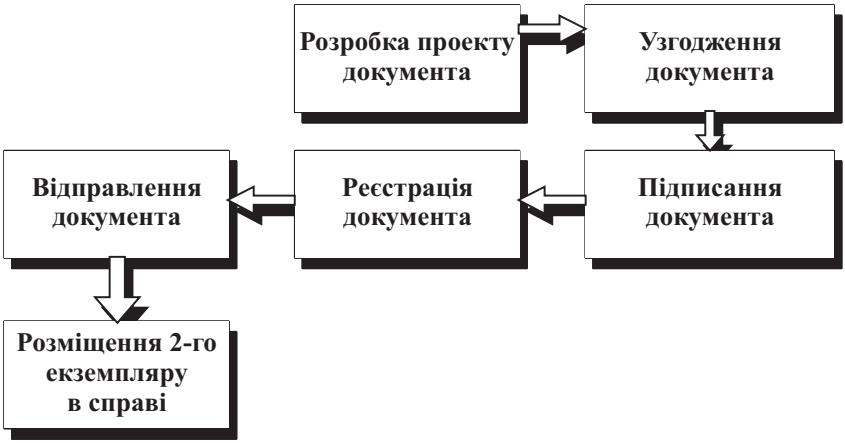
Рішення про подальше використання конфіденційного документа визначається його значенням і практичною цінністю. Залежно від цього конфіденційні документи можуть:

1.) - використатися надалі ;
2.) - передаватися в архів на зберігання;
3.) - знищуватися.

Всі ці дії повинні виконуватися з дотриманням вимог до конфіденційних документів.

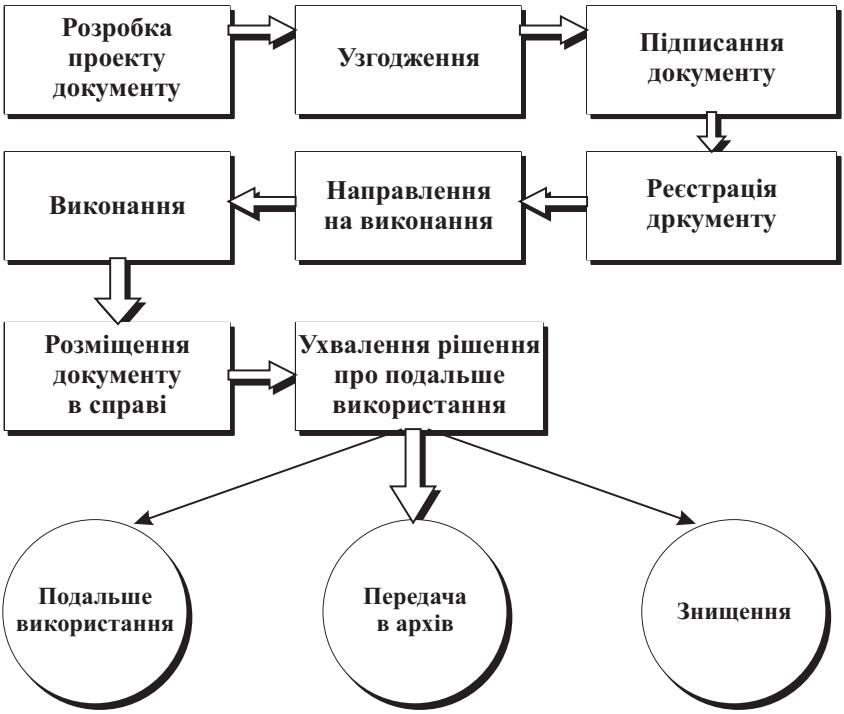
Робота з конфіденційними вихідними документами включає наступні етапи (мал. 5):

- розробка проекту документа;
- узгодження документа;
- підписання документа;
- реєстрація документа;
- відправлення документа.



Мал. 5. Порядок роботи з конфіденційними вихідними документами

Проект вихідного конфіденційного документа розробляється виконавцем документа в 2-х екземплярах і по необхідності согласовывается з іншими фахівцями фірми. Далі проект документа надається на підпис керівникові фірми. Після підписання документа, він реєструється співробітником конфіденційного діловодства в журналі (картці) реєстрації вихідних конфіденційних документів. Розсилання конфіденційних документів здійснюється згідно підписаних керівником списків з обов'язковою вказівкою облікових номерів відправлених документів. Порядок роботи з конфіденційними внутрішніми документами показаний на мал. 6.



Мал. 6. Порядок роботи з конфіденційними внутрішніми документами

Видача й повернення конфіденційних документів повинні вчасно відбиватися в журналі обліку й видачі конфіденційних документів (мал. 7).

№ п/п	Номер документу	Дата видачі	Короткий зміст (найменування)	Кількість листів		Кому виданий (П. І. Б.)	Підпис в отриманні	Відмітка про повернення (підпис і дата)	Примітка
				Листів	Екземплярів				

Мал.7. Журнал обліку видачі конфіденційних документів

При одержанні конфіденційного документа співробітник повинен звірити номер отриманого документа з його номером у журналі, перевірити кількість аркушів і розписатися за отриманий документ. При поверненні конфіденційного документа співробітник конфіденційного діловодства повинен звірити номер цього документа з номером у журналі, перевірити кількість аркушів документа й у присутності співробітника, що повертає документ поставити в журналі (у відповідній графі) свій підпис і дату повернення документа.

Всі папки з конфіденційними документами й журнали їхнього обліку вносяться в номенклатуру справ фірми.

По закінченні кожного року керівником фірми створюється комісія, що повинна:

1.) - перевірити наявність конфіденційних документів;

2.) - визначити конфіденційні документи для архівного зберігання;

3.) - визначити конфіденційні документи, що підлягають знищенню.

Архівне зберігання конфіденційних документів проводиться в опечатаних коробках, у приміщеннях, що виключають несанкціонований доступ сторонніх осіб. На конфіденційні документи, відібрані до знищення комісією, становить акт. Акт затверджується керівником фірми.

У випадку втрати конфіденційного документа керівником фірми створюється комісія, що проводить розслідування по факті втрати даного документа. За результатами роботи комісії керівником фірми приймається рішення про залучення до відповідальності осіб винних у втраті конфіденційного документа.

Таким чином, представлений матеріал у дуже скороченому виді дає певні рекомендації з організації конфіденційного діловодства на підприємстві, що безсумнівно допоможе співробітникам служби безпеки захистити конфіденційну інформацію в цілому.

Загальні заходи з захисту конфіденційної інформації

1. Документування дій осіб, затриманих за адміністративну провинність.

Маються на увазі перш за все такі адміністративні правопорушення, які підривають економічну безпеку підприємства (наприклад, дрібні розкрадання) і через певні обставини не можуть бути виявлені охоронцями. Протиправні дії адміністративних правопорушників ретельно документуються (довідки, пояснення, акти і т.д.) і передаються в той орган, в компетенцію якого входить їх розгляд. Особливу увагу при цьому слід звернути на те, щоб при затриманні правопорушника були присутні очевидці, чия об'єктивність не береться під сумнів (наприклад, не рекомендується запрошувати як очевидця співробітника СБ).

2. Виявлення осіб з числа персоналу, що сприяють злочинним елементам (що не працює на підприємстві) в здійсненні ними злочинів.

Оскільки злочинці при реалізації своїх задумів прагнуть привернути до негласної співпраці працівників підприємства, то цій категорії персоналу з боку контррозвідки повинна бути приділена найпильніша увага. З цією метою складається список потенційних помічників злочинцям, і з ними проводиться робота із застосуванням законних методів. Результатом такої роботи повинні бути або документування злочинних дій співробітника підприємства, або відміна його до відмови від скоєння злочину.

3. Викривання економічних (промислових) шпигунів з числа персоналу.

Встановлення і викривання економічних шпигунів, тобто осіб, що використовують незаконні методи, які приводять до матеріального збитку підприємства, є найважливішою функцією контррозвідки. При цьому контррозвідники зобов'язані використовувати тільки законні методи і засоби. Особливу увагу слід приділяти документуванню діяльності шпигунів, що дозволить згодом привернути їх до цивільно-правової, а в деяких випадках і до кримінальної відповідальності.

4. Створення умов, що виключають підслуховування розмов в службових кабінетах.

Реалізація цієї функції має виняткове значення, оскільки дозволяє керівництву підприємства, що охороняється, зберегти не тільки комерційну таємницю, але і будь-яку конфіденційну інформацію службово-

го характеру. Створити умови, що виключають підслуховування розмов, можна за допомогою організаційних і технічних заходів.

До організаційної групи заходів входять інструктажі, розробка пам'яток і т.д. Технічні заходи включають систематичні обстеження службових приміщень з метою виявлення підслуховуючих пристроїв. Особливу увагу слід звернути на створення умов, що виключають підслуховування, при проведенні переговорів з діловими партнерами.

5. Встановлення обставин розголошування відомостей, (складових комерційної таємниці.)

Комерційною таємницею стає тільки та інформація, яка затверджена керівництвом підприємства в «Переліку відомостей, складових комерційну таємницю підприємства» і оголошена під розписку всім причетним до неї співробітникам. Під розголошуванням комерційної таємниці розуміється навмисна або ненавмисна передача (усно або письмово), без згоди власника (власника) або керівника, визнаних в установленому порядку такий, стороннім особам або невизначеному коло осіб.

Заходи по внутрішній безпеці підприємства

Заходи щодо забезпечення внутрішньої безпеки керівник служби безпеки повинен будувати за наступною схемою:

- Ясно представляти можливі джерела погроз і їх мотиви, виходячи з положення в світі бізнесу, стану справ, величини фінансових коштів, можливої наявності крупних боргів, ділових і особистих взаємин з конкурентами.
- Дотримуватися обережності і пильність, вивчати навколишнє оточення і людей.
- Особливу увагу приділяти вивченню і спостереженню за найбільш вірогідними небезпеками.
- Виробити і дотримувати певні правила поведінки керівництва та працівників, направлені на забезпечення особистої безпеки, зробивши їх складовою частиною способу життя.
- Відпрацювати правила безпечної поведінки для всіх працівників підприємства та членів їх сімей.
- При виявленні ознак небезпеки негайно просити допомоги у правоохоронних органів. Відпрацювати правила безпеки керівника при діловому і особистому його спілкуванні, при пересуванні на транспорті і пішки, удома, на службі, на відпочинку, у відрядженнях. Навчити (кон-

тролювати) правила безпеки при використанні керівником автомашини.

- Знати, як поводитися у разі викрадання керівника. Навчити керівника та службовців навикам безпеки при виявленні вибухових пристроїв.
- Вивчити ознаки підготовлюваних кримінальних злочинів: замовленого вбивства, викрадання, психологічної дії.

Ці ознаки можна виявити, якщо знати, що вони із себе вдають.

4.3. Службові розслідування (на прикладі – при надходженні сигналу про втрату конфіденційних документів).

Керівництву фірми необхідно встановити порядок, при якому кожен випадок втрати конфіденційних матеріалів, розголошування або можливого розголошування фірмових секретів, порушення вимог Положення про конфіденційну інформацію негайно докладався із Службу безпеці, яка зобов'язана оперативно почати розслідування. При цьому американські фахівці, наприклад, виходять з наступного: при отриманні сигналу про втрату (розголошуванні) будь-який конфіденційний матеріал, який не виявлений в місці зберігання, вважається втраченим, а фірмовий секрет -разглашенным, поки розслідуванням не буде встановлено інше.

Отримавши повідомлення про втрату конфіденційних матеріалів, розголошуванні або можливому розголошуванні фірмових секретів, порушенні вимог Положення про конфіденційну інформацію, служба безпеки приймає заходи для встановлення всіх обставин по отриманому сигналу.

1.) На початковому етапі розслідування служба безпеці зобов'язана:

- перевірити достовірність отриманої інформації,
- переконатися в тому, що втрачені матеріали або розголошені відомості дійсно відносяться до категорії конфіденційних,
- опитати осіб, що мали безпосереднє відношення до того, що трапилося, втраченим документам (розголошеним відомостям).

2.) Уточнюються наступні питання:

- що конкретно відбулося, де і коли,
- хто повідомив про той, що трапився, кому і коли,

- про які конкретні матеріали (інформації) йде мова, ступінь їх конфіденційності,

- наскільки втрата документів (розголошування відомостей) завдає збитку фірмі, - дані на всіх осіб, що мали відношення до цих документів (інформації),

- коли, як довго і за яких обставин ці конфіденційні документи (інформація) могли стати уразливими для несанкціонованого доступу до них.

- дані на осіб, що можливо дістали через ті або інші причини несанкціонований доступ до конфіденційних матеріалів (інформації),

- які заходи були прийняті, щоб захистити фірмові секрети і мінімізувати збиток до того, як почалося розслідування, коли і ким були прийняті ці заходи (термінова перевірка наявності інших документів, посилення захисних заходів при зберіганні, зміна комбінацій на замках сейфів, оновлення паролів доступу до ЕОМ і т.п.),

- чи загублений конфіденційний документ або просто не врахований (фірмовий секрет викладений в документі без грифа секретності).

Якщо в результаті розслідування встановлено, що дійсно має місце факт втрати конфіденційного документа, розголошування фірмових секретів або серйозного порушення вимог Положення про конфіденційну інформацію, служба безпеці готує рапорт першому керівникові фірми про той, що трапився з викладом результатів вже проведеної перевірки і комплексу намічаних подальших заходів.

Після закінчення розслідування служба безпеки також докладає першому керівникові фірми рапорт, в якому детально висловлює фабулу справи (зокрема, по переліку питань, викладених вище), настановні дані ідолжность особи, винної в тому, що трапився, його коротку характеристику, оцінку збитку, понесеного фірмою із-за того, що відбувся, прийняті і пропоновані заходи по локалізації збитку і недопущенню подібних випадків в майбутньому, пропозиції про покарання винного.

У зв'язку з вищевикладеним необхідно зробити наступне зауваження: набагато простіше і дешевше запобігти втраті конфіденційних документів або розголошуванню фірмових секретів, чим проводити комплекс спеціальних заходів за фак Перш за все том надзвичайної події, що трапилася, і мінімізації матеріального і морального збитку..

Таким чином, виключно важливо розробити Положення про конфіденційну інформацію і докладну Інструкцію про роботу з

конфіденційними документами, вимоги яких обов'язкові для виконання всіма співробітниками фірми.

Правильна організація конфіденційного діловодства на фірмі є складовою частиною комплексного забезпечення безпеки інформації і має важливе значення в досягненні мети її захисту. Як відомо, фахівці, що займаються в області інформаційної безпеки стверджують, що порядка 80% конфіденційної інформації знаходиться в документах діловодства. Тому питання конфіденційного документообігу у фірмі поза сумнівом грають важливу роль в досягненні нею економічних успіхів.

Деякі рекомендації, що дозволяють упорядкувати роботу на фірмі з конфіденційними документами будуть розглянуті в окремих темах та на семінарах (практичних заняттях).

4.4. Забезпечення кредитної політики банку, фірми, тощо. (Вивчення надійності й платоспроможності клієнтів)

В кінці XX століття, серед різних прошарків населення набуло широке поширення в Україні -практика неповернення боргів, невиконання договірних зобов'язань, шахрайства, відсутності централізованих державних інформаційно-довідкових систем про надійність і платоспроможність суб'єктів ринку, недотримання комерційної етики, проблема вивчення надійності й платоспроможності клієнтів, особливо тих, хто бере кредити.

Головними умовами встановлення ділових відносин між суб'єктами ринку є гарне знання свого клієнта й постійна його перевірка. У країнах з розвитий ринковою економікою збір, аналіз, узагальнення, нагромадження й використання інформації про надійність потенційних партнерів по бізнесі, їхній фінансовій заможності й сумлінності становлять відпрацьовану систему перевірки комерційних контрагентів.

Важливе значення надається при цьому добуванню й використанню інформації про застосування потенційними партнерами й конкурентами несумлінної конкуренції.

Відомості про їх виробничу, збутову, науково-дослідну, фінансову й іншу діяльність утримуються в різних каталогах, рекламних проспектах, бюлетенях, довідниках, прейскурантах.

Критеріями оцінки репутації підприємницької структури прийняті, згідно даним досить авторитетних у світі з журналів "Форчун" (США) і "Економіст" (Великобританія), що випливають показники:

- якість керування й вироблених товарів і послуг;
- фінансовий стан; використання ресурсів;
- уміння залучати талановитих людей; довгострокові капіталовкладення;
- здатність до інновацій (нововведенням);
- відповідальність перед суспільством і природою.

Банки й фірми повинні вивчатися з погляду правового, комерційного, майнового й фінансового стану. У цих цілях рекомендується створення комісії в складі юриста, фінансиста, зі служби безпеки й ін. Існують різні методики збору інформації про клієнта.

Загальним для них є складання запитальника для з'ясування відомостей, що характеризують клієнта й банк, що представляє їхню фірму. Звичайно запитальники розробляють у вигляді інформаційних карт на фізичних й юридичних осіб.

1.) Інформаційна карта на фізичну особу включає наступні відомості:

- прізвище, ім'я, по батькові;
- дату народження;
- місце народження;
- національність;
- громадянство;
- адреса (поштовий індекс);
- телефон; телекс; факс; телетайп;
- час, коли краще дзвонити;
- дані паспорти, закордонні паспорти, номер водійського посвідчення, посвідчення особи; категорію обліку в ОВД;
- прикмети зовнішності;

- відомості про родину, близькі зв'язки,
- посада;
- функціональні обов'язки;
- утворення; професія; попередній досвід роботи;
- рівень зарплати;
- рівень матеріальної забезпеченості;
- житлові умови;
- корінний житель міста або недавно переїхав у нього;
- стиль життя (елітарний, богемний, спортивний, молодіжний);
- особисті якості (амбіційність, авторитарність, імпульсивність і т.п.).
- місце розташування офісу (район, адреса, окремий будинок, частина будинку, окремий поверх, кілька кімнат, приватна квартира);
- статус клієнта (постійний; хоче стати постійним; раніше був вашим клієнтом; сторонній);
- оцінка клієнтом власного бізнесу (процвітаючий, що дає середній дохід, поки без успіхів);
- психологічний стан під час відвідування банку, фірми.

В інформаційну карту входять також додаткові відомості:

- ріст (низкий-до 165 сантиметрів, середній - 165-175 сантиметрів, високий- 176-185 сантиметрів, дуже високий - 186 сантиметрів і більше);
- статура (повне, середньої вгодованості, сухорляве);
- тип особи (слов'янський, кавказький, середньоазіатський, прибалтійський, єврейський, циганський);
- колір особи (блідий, жовтий, червоний, звичайний, смаглявий);
- колір очей (блакитні, зеленуваті, карі, сірі, чорні, інший);
- колір волось (рудий, світлий, сивий, із проседью, темно-русявий, чорний, інший);
- форма волось (кучеряві, прямі, інша);
- довжина волось (довгі, середньої довжини, короткі, коса, інша);
- лисина (залисини, лобова, лобово-тім'яна, макушечная, повне облисіння);

- особливості мови (швидка, повільна, невиразна, шепелява, гаркава, із заїкуватістю, з акцентом, інші).

Особливості, Що Кидаються в очі:

- особи (асиметричне, надмірно подовжене, інше);
- чола (більші надбрівні дуги, лобові ямки, сильно скошений, вузький, інший);
- брів (асиметричні, зрослі, інші);
- носа (з горбочком, кривій, інший);
- око (більмо, косоокість, носіння окулярів, відсутність лівого ока, відсутність правого ока, протез ока, інші);
- губ (верхня виступаюча, заяча губа, косі, нижня виступаюча, обидві виступаючі; постійно напіввідчинені, товсті, тонкі, інші);
- зубів (більші, криві, дрібні, рідкі, із щілиною між верхніми передніми зубами, інші);
- вух (відстовбурчена, прилягаюча, зросла мочка, інші);
- підборіддя (виступаючий, дуже вузький, дуже широкий, роздвоєний, скошений назад, з поперечною борозною, з ямкою, інший);
- шиї (дуже довга, дуже коротка, з виступаючим кадиком, інша);
- тулуба (дуже вузькі плечі, дуже широкі плечі, з горбом, сутулий, інше);
- ходи (вразвалку, клишаве, повільна, носіння тростини, дуже швидка, кульгавість, інші).

Особливі прикмети (бородавки, ластовиння, родимки, рідні плями, сліди опіку, сліди віспи, шрами, інші);

- відсутність кінцівок (лівої руки, лівої ноги, правої руки, правої ноги, пальців руки);
- дата уведення (корекції) інформації.

2.) Інформаційна карта на юридичну особу (банк, фірму) включає наступні відомості:

- час роботи установи;
- коли приступилися до діяльності;
- основні засновники;
- статутний капітал;

- юридична адреса, чи збігається він з адресою офісу клієнта;
- організаційно-правова форма;
- основні керівники (прізвища, імена, по батькові, посади, номери їхніх телефонів і т.д.);
- особа, що приймає рішення;
- число працюючих;
- основний профіль і види діяльності структури;
- оцінка загального стану справ;
- наявність дочірніх підприємств і філій;
- успіхи;
- основні партнери;
- нерухома власність;
- структура;
- у яких банках перебувають рахунки.
- хто здійснює аудита;
- коли востаннє брали кредит і де;
- чи виникали раніше труднощі з поверненням кредитів;
- на що планується використати кредит;
- бажана сума кредиту, наскільки вона обґрунтована;
- можливе забезпечення кредиту;
- імовірний строк і порядок погашення;
- відсоток по позичці.

На першому етапі встановлення ділових відносин проводиться бесіда керівництва банку, фірми з потенційними партнерами. Якщо партнери солідні, у бесіді, як правило, бере участь начальник служби безпеки. Ознайомлювальну бесіду із клієнтами іншої категорії в банках звичайно проводять співробітники кредитного підрозділу (без участі представника служби безпеки). Вони повинні навчитися розташовувати до себе клієнтів й одержувати максимум відомостей, що цікавлять, про їх. Після зустрічей із клієнтами необхідно становити письмовий звіт, що неодмінно повинен заставлятися в досьє на потенційного партнера.

Обов'язково варто побувати в тих державних організаціях, де реєструвалося підприємство, і переконатися в реальності правового оформлення банку, фірми. У той же час потрібно неодмінно відвідати дану комерційну структуру. Під час її відвідування треба:

* - переконатися в наявності банку, фірми по зазначеній адресі;

* - познайомитися з їхніми керівниками;

* - вивчити оригінали установчих документів підприємства, балансового звіту за попередній рік і за минулий час поточного року, реєстраційних посвідчень, ліцензій, патентів й ін.;

* - неодмінно оглянути офіс, звернути увагу на існуючу в ньому обстановку (інтер'єр, культура спілкування співробітників, їхній зовнішній вигляд, манери, лексика й т.д.). Надалі клієнт зобов'язаний представити пакет документів, що досліджується з обліком раніше отриманої інформації.

У пакет документів звичайно входять:

- установчі документи - устав й установчий договір;
- копії балансів за останній рік й останній звітний період поточного року;
- техніко-економічне обґрунтування продукту або програми;
- заявка на кредитування;
- пояснювальна записка;
- ліцензія на вид діяльності (якщо він ліцензується);
- сертифікати на випуск продукції й т.д.

На заключній стадії, перед ухваленням рішення про укладання договору про кредит, поставку продукції або товару, проводять додаткову перевірку отриманих документів і відомостей. Для цього використають:

- свою інформаційну базу (при її наявності), що може містити дані про сумнівних клієнтів, рейтинг потенційного партнера, його фінансовому стані, можливій наявності кримінальної "даху", його неблагополучному стані й т.д.;
- інформаційні зв'язки співробітників служби безпеки (охоронної фірми), керівників і надійних службовців банку, фірми в різних державних і недержавних структурах (в органах влади й керування, правоохоронних відомствах, спеціальних службах, підприємницьких і банківських колах, засобах масової інформації, науковому світі, служ-

бах безпеки банків; і фірм, охоронних фірмах, інформаційних центрах); інформаційні можливості колишніх клієнтів банку, фірми й т.д.

Отриману інформацію перевіряють, аналізують й оцінюють. На цій основі ухвалюють рішення щодо вступі або невступі банку, фірми в договірні відносини із клієнтом.

Діяльність служби безпеки по розробці й реалізації кредитної політики банку, фірми

Як виявляється з аналізу основних проблем забезпечення безпеки підприємницької діяльності, до їхнього числа ставиться й неповернення кредитів. У середньому близько 80 % видаваних кредитів безповоротні в силу різних причин. Певна частина кредитів, видаваних за хабар, споконвічно не може бути повернута.

Вивчення й узагальнення вітчизняного досвіду кредитної політики банків свідчить про те, що **головними причинами неповернення боргів** (крім заздалегідь безповоротних) є:

- відсутність або поверхнева попередня перевірка ссудозаемщиков;
- недостатньо кваліфіковане юридичне проробление кредитних договорів;
- виключення в нерідких випадках служб безпеки банків і фірм із процесу розробки й реалізації їхньої кредитної політики;
- недосконаліть законодавчої бази, що регулює кредитну політику в країні;
- некомпетентність деяких керівників, що приймають рішення про видачу кредитів, і допуска ними при цьому надмірний ризик.

На етапі розробки кредитної політики банку основні завдання його служби безпеки полягають в участі разом з відділом кадрів у підборі, навчанні й розміщенні співробітників кредитних підрозділів банку.

Попередньо необхідно:

а) зажадати від кандидатів на роботу в кредитний підрозділ максимально повний комплект документів;

б) ретельно перевірити майбутніх співробітників у ході бесід, відвідування колишніх місць роботи, навчання;

в) перевірити по каналах МВС можливість наявності судимості або знаходження в розшуку;

г) неодмінно провести їхнє тестування по якісних методиках, щоб визначити особисті й ділові якості згідно професиограммам.

Крім того, служба безпеки бере участь в організації **інформаційно-аналітичного забезпечення кредитної політики банку**. Основна увага варто приділяти при цьому постійному збору й аналізу інформації з наступних питань:

а) стан і тенденції розвитку обстановки на ринку банківських послуг;

б) кримінальні погрози, прояви й хитрування злочинних елементів у кредитній сфері; в) відомості про сумнівних клієнтів (юридичних і фізичних особах);

г) зловживання співробітників банку в кредитній сфері (хабара, шахрайство, розголошення комерційної таємниці, спроби знайти доступ до конфіденційної інформації й т.буд.).

У цьому зв'язку надзвичайно важливе здійснення комплексу заходів щодо підготовки персоналу банку до дій у кризових ситуаціях, що виникають у результаті неповернення кредиту.

У процесі реалізації кредитної політики банку служба безпеки бере участь у рішенні наступних питань:

- робота з відвідувачами - потенційними позичальниками;
- вивчення представленого клієнтами пакета документів за заявкою на кредит;
- вивчення надійності клієнта й ступені ризику по можливій видачі позички;
- структурування позички, підписання кредитного договору;
- кредитний моніторинг;
- стягнення заборгованості по кредитних договорах.

При структуруванні позички й підписанні кредитного договору служба безпеки залучається до розробки компромісного варіанта кредитного договору, що задовольняє обидві сторони, а також до підготовки доповіді керівництву банку про план дій по відстеженню виконання кредитного договору (якщо він укладений на велику суму).

У процесі кредитного моніторингу, що у банківській практиці, як правило, не використається, службі безпеки необхідно постійно контролювати виконання умов кредиту ссудозаемщиком. Такий контроль,

здійснюваний разом зі співробітниками кредитного підрозділу, повинен бути спрямований на виявлення ознак виникнення в ссудозаемщика проблем з поверненням боргу.

Зовнішні прояви виникнення утруднень у ссудозаемщика по поверненню кредитів можуть бути наступними:

- погіршення фінансового становища;
- складності у взаєминах з партнерами, податковими органами, кримінальними елементами.

Кредитний моніторинг ссудозаемщика, здійснюваний службою безпеки, дозволяє вирішити два завдання:

1) - уберегти ссудозаемщика від банкрутства;

2) - вчасно припинити його подальше кредитування, якщо воно проводиться по кредитній лінії (вроздріб).

Аналогічну роботу з відстеження положення справ службі безпеки важливо проводити й у відношенні гаранта кредиту - банка, компанії, фірми й т.д.

Дуже відповідальною і складною є діяльність служби безпеки разом зі співробітниками кредитного і юридичного підрозділів банку по поверненню кредиту служба безпеки банку в таких випадках зобов'язана здійснювати комплекс наступних заходів:

1. Надання психологічного тиску на несумлінного позичальника різними засобами: погрозою внести боржника в "чорні списки" АУБ й у бази даних про шахраїв у МВС; попередженням про проведення кампанії антиреклами в засобах масової інформації; наданням вигідного впливу на боржника через загальних партнерів, його акціонерів і серйозних клієнтів; створенням доказової (свидетельской) бази й фіксуванням слідів протиправної діяльності боржника перед обігом банку в суд, арбітражний суд, третейський суд; підтримкою ділових контактів з державними правоохоронними органами на стадії порушення кримінальної справи, пред'явлення претензій і т.д.

2. Визначення ймовірного використання позичальником кримінального впливу на кредитор.

3. Перехід служби безпеки на посилений режим роботи при підтвердженні сигналу про підготовку позичальника до силових акцій проти банку.

При цьому здійснюються:

- активізація роботи з позичальником і по виявленим у якості пов'язаних з ним злочинним елементам; посилення роботи зі співробітниками банку, у поводженні яких відзначені моменти, що насторожують;
- підвищення рівня фізичної безпеки банку, безпеки каналів зв'язку, перевезень фінансових засобів і коштовних вантажів;
- доозброєння служби безпеки;
- посилення особистої охорони керівників банку;
- активізація ділових контактів з державними правоохоронними органами, насамперед з тими, які розташовані поблизу банку;
- додатковий інструктаж персоналу банку з питань безпеки й тактики поводження у випадку злочинного зазіхання;
- перевірка наявності засобів першої медичної допомоги.

4. Запровадження в дію плану роботи банку в кризовій ситуації, якщо обстановка загострюється. Про злочинну акцію, що готується, офіційно інформуються державні правоохоронні органи, яким передається вся зібрана інформація.

Служба безпеки може сприяти співробітникам юридичного відділу банку по поверненню кредиту правовими методами.

4.5. Внутрішнє шахрайство на підприємстві

Виявлення:

Наступний етап у цій нелегкій боротьбі розумів й аналітичних здатностей – це **виявлення шахрайства**, тобто проведення службами безпеки й інших підрозділів (фахівцями) підприємства, що мають контрольні функції, комплексу оперативних й адміністративних заходів для визначення ознак неправомірних дій. Зрозуміло, що, якщо шахрайство відбулося, це не може бути приховано безвісти. Хоча є такі підприємства, де облік і контроль (основні принципи соціалізму?) на яких поставлено так, що "це" може бути приховано майже безвісти. Ну, а де все обстоит більш-менш нормально, напевно повинне бути щось, за що можна зачепитися відповідному підрозділу.

Почнемо з того, що відповістимо на запитання: як служба безпеки (СБ) може довідатися про факти що готується або уже зроблене шахрайства?

1. Співробітник підприємства може розповісти про наявних у нього підозрах безпосередньому керівникові, що цю інформацію передасть у СБ (от вона - лояльність!).

2. Співробітник може повідомити про свої підозри прямо в СБ.

3. Керівник СБ повинен «довідатися» про необхідну інформацію зі звітів проведення інвентаризаційних, ревізійних, аудиторських й інших контрольних і перевірочних заходів.

4. З відомостей діючої лінії для прийому анонімних повідомлень, так називаної "гарячої лінії". При цьому використається автовідповідач, абонентська або поштова скринька, ящик для листів на території підприємства, прийом повідомлень на пейджер і тому подібні способи прийому анонімних й, може бути, авторизованих послань.

5. У СБ може надійти інформація із зовнішніх джерел, так чи інакше замішаних у здійсненні дій проти власності підприємства.

6. Керівник або інший співробітник СБ самі виявлять ознаки шахрайства при виконанні своїх обов'язків.

До речі, ні за яких умов співробітники й менеджери, що довідалися про протизаконні дії своїх колег, не мають права самостійно розмовляти з підозрюваними в здійсненні шахрайства, всі дії ведуться тільки через СБ.

Звідки може прийти інформація, що цікавить, ясно, тільки від джерела, треба проаналізувати яка інформація вас, (керівника СБ), зацікавить?

Безсумнівно та, котра може містити:

а) - ознаки здійснення шахрайства;

б) - ознаки способів приховання;

в) - ознаки реалізації викраденого (привласненого);

г) - ознаки наслідків здійснення.

Зі здійсненням і наслідками зрозуміло, а от при чому тут приховання? Шахрайство тим і відрізняється від грабежу або крадіжки, що шахраї, тим більше "власні", приховують свої дії. А що стосується реалізації викраденого, то тут існує закономірність: якщо співробітник розбагатів на грошах своїх роботодавців, то по його образі життя, що змінився, це незабаром буде видно.

Класифікуємо ознаки здійснення, про які, будемо вважати, уже відомо. Це потрібно для того, щоб звузити коло винних осіб і по цих озна-

ках, з відомою часткою ймовірності, визначити так званий «рівень причетності».

Досвід показує, що правильно розрізняти такі рівні:

1. Рівень найманих робітників підприємства (РНР);

2. Рівень осіб, що приймають рішення (ОПР), тобто верхня й вища ланка з підприємства;

3. Рівень зовнішній, тобто сторонні організації.

Рознесення ознак по рівнях, зрозуміло, досить умовне. Спільники, а той ініціатори, можуть бути й ззовні, більше того, найчастіше так і буває.

Рівень найманих робітників (РНР)

Ознаки здійснення дій, ініціаторами й/або виконавцями яких вони є. Відхилення в первинному бухгалтерському обліку:

- прострочені проводки, подвійні оплати;
- збіг платіжних реквізитів замовників й одержувачів платежів;
- не представляють змісту послідовності документів;
- сумнівні написи на документах від руки;
- надання копій, а не оригіналів документів;
- занадто багато дебіторських або кредиторських нагадувань;
- недостачі або перевищення по касі;
- здійснення платежів з істотним запізнюванням;
- і багато інших ознак, можливість розібратися в які краще надати кваліфікованим аудиторам.

Відхилення від середніх (нормальних) значень величин яких-небудь показників:

- несподівані недостачі або надлишки;
- збільшення залишків;
- відхилення від специфікацій;
- незрозумілі розбіжності у фізичних характеристиках;
- надлишкові закупівлі;
- і багато інших ознак, що ставляться або до невідповідності даних в облікових документах у порівнянні з фактичним положенням, або до яких-небудь нестандартних тенденцій.

Взагалі всі маніпуляції шахраїв бухгалтерів, касирів й інших осіб, що мають право виконувати бухгалтерські проводки, як правило, зводяться до внесення змін в облікові регістри.

1. Для запобігання такого роду шахрайства необхідно дозволити доступ до здійснення бухгалтерських проводок тільки бухгалтерові, що виконує цю роботу.

2. Наприкінці кожного робочого дня повинні бути роздруковані й завірені підписами двох незалежних друг від друга працівників підприємства всі журнали ордерів або журнал господарських операцій.

Рівень осіб, що приймають рішення (ОПР)

Відхилення яких-небудь підсумкових фінансових показників від середніх (нормальних) величин (тенденцій):

- збільшення доходів при зменшенні матеріально-виробничих запасів;
- збільшення доходів при зменшенні обороту по касі;
- збільшення запасів при зменшенні кредиторської заборгованості;
- збільшення числа продажів при збільшенні ціни за одиницю продукції;
- збільшення обороту при скороченні залишків;
- збільшення запасів при зменшенні витрат на обслуговування складів;
- непояснені зміни в балансовій звітності;
- погіршення якості прибутку (по ефективності);
- недостатність основного капіталу;
- висока заборгованість, велика питома вага накладних витрат;
- більше швидкий ріст витрат у порівнянні зі зростанням доходів;
- труднощі в стягненні дебіторської заборгованості та інші проблеми, пов'язані з рухом фінансів;
- і багато інші, пов'язані з відстеженням динаміки підсумкових величин, як правило, сторонніми аудиторськими бюро.

Шахраї цієї групи в основному роблять розкрадання шляхом надання необгрунтованої знижки до ціни продукції або товару, шляхом відвантаження продукції до початку її переоцінки й ін., (при продажі), необґрунтованого завищення ціни (при покупці - змова з постачальником).

Для виявлення таких зловживань необхідно передбачити в базах даних (БД) по угодах (договорам, контрактам) індексування за різними критеріями й регулярно аналізувати матеріали БД за цими критеріями, зокрема :

1.) - по даті відвантаження;
2.) - за ціною;
3.) - по величині партії;
4.) - по номенклатурі товару;
5.) - по конкретному клієнті й ін.

Надалі протягом досить репрезентативного (представницького) періоду, наприклад, за квартал, аналізуються всі господарські операції по конкретному клієнті або по конкретному товарі. Якщо за цей проміжок часу зафіксовано, наприклад, необґрунтоване відхилення ціни продукції від її реального значення з урахуванням індексу інфляції - призначається службове розслідування причин (некомпетентність або намір).

Крім того, для полегшення такого аналізу рекомендується на підприємстві мати затверджений стандарт, що закріплює за кожним типом проводки властиві тільки йому ознаки. Наприклад, проводки, пов'язані з реалізацією продукції, повинні містити реквізити споживача (адреса, телефон, факс) і інші ознаки, по яких видно угоди з конкретним споживачем по конкретній групі товарів.

Непояснені відхилення (аномалії) у діяльності підприємства:

- робота на грані кризи;
- незвичайні або великі нібито вигідні угоди наприкінці звітного періоду;
- залежність від виробництва, продажу лише одного-двох виробів (послуг);
- участь підприємства у великих судових справах;
- зайво ускладнена структура підприємства;
- відсутність підрозділу внутріфірмового аудита;
- прихильність до высокорискованным операцій;
- часті зміни в рядах вищої управлінської ланки й серед членів Ради директорів;
- великі угоди з родинними партнерами;
- і багато інших ознак проблем, рішення яких залежить від певних осіб.

Ознаки шахрайства ЛПР із інвестиціями. При аналізі принципово не виявляються, тому що дана інформація не завжди доступна навіть керівникам СБ. Має практичний характер у випадку, якщо керівник СБ,

наприклад, якогось холдингу, ставить під контроль використання інвестицій у філії або відділенні:

- використання інвестицій для сфери підприємництва, нової й незвичайної для даної місцевості, ринку;
- для дій з інвестиціями, що раніше супроводжувалися скандалами або банкрутствами;
- для підозрілих і ризикованих проектів;
- відсутність чіткої обґрунтованості даного способу розміщення інвестицій;
- шикарний спосіб життя керівників, що вказує на "інвестиційний слід" джерела доходу;
- і інші.

Зовнішній рівень

Приведемо приклади таких фактів або тенденцій взаємин зі сторонніми партнерами й іншими організаціями, аналіз яких повинен керівника СБ насторожити. Перелік, зрозуміло, далеко не повний, його зміст залежить від конкретної специфіки й масштабів діяльності підприємства. Необхідно тільки звернути вашу увагу на те, що нижченаведені проблеми, найімовірніше , можна віднести до якихось навмисних дій з боку найвищого керівництва.

Юридичне забезпечення діяльності:

- ведення великих судових процесів;
- часті зміни юрисконсультів.

Аудиторське забезпечення діяльності:

- часті зміни зовнішніх аудиторів;
- відмова або затримки в наданні аудиторам необхідної інформації;
- відсутність підрозділу або фахівця внутріфірмового аудита;
- відмова аудитора від винесення судження або незгоди з даними наданих фінансових документів.

Відносини з ліцензійними, податковими й іншими фіскальними органами:

- відкликання або проблеми з обслуговуванням ліцензій;
- часті перевірки з боку контрольних органів;
- постійні проблеми з податковими органами й ін.

Фінансове забезпечення діяльності:

- використання декількох банків;

- нездатність фірми забезпечити фінансування шляхом одержання кредитів або позик й ін.

Відносини з родинними фірмами:

- угоди винятково (або майже винятково) між родинними (вхідними в одну "родину") фірмами.

Відносини з партнерами:

- постійний тиск до злиття, продажу або поглинанню інших фірм;

- реорганізація структури відносин між партнерами, що послабляє позиції вашого підприємства.

Відносини із замовниками або постачальниками:

- підозріло велика кількість нових замовників або постачальників;

- наявність замовників або постачальників, що не пройшли певні перевірки й ін.

Наявність постійного тиску з боку політичних, екологічних організацій, засобів масової інформації, профспілки й суспільної думки.

Як правило, завжди є присутнім кілька ознак різних рівнів, правильне синтезування яких дозволяє найбільше точно виявити й кваліфікувати вид шахрайства. А це - запорука успіху надалі розслідуванні.

Ознаки способів прихованого шахрайства

Розглянемо проблеми, пов'язані з використанням отриманої інформації, що містить ознаки способів приховання шахрайства.

Одним з напрямків діяльності СБ повинна бути постійна кропітка робота, пов'язана з пошуком підроблених і виправлених документів або фактів навмисної зміни стану яких-небудь матеріальних активів саме з метою своєчасного знаходження таких. Для цього постійно організуються різного роду перевірки й контрольні заходи. При будь-яких таких перевірках у складі комісій повинні бути фахівці зі СБ.

При одержанні шуканої інформації даний факт засвідчується відповідним актом, при необхідності членам комісії дається вказівка зберігати конфіденційність происшедшего на певний час. Подальші дії СБ по розробці даної інформації, тобто визначенні причин приховання, є вже розслідуванням.

Також необхідно детально зупинитися й на проблемах, пов'язаних з одержанням і використанням інформації про ознаки реалізації викраденого.

Як уже говорилося, злочинець, що викрав матеріальні цінності або гроші, повинен буде позбутися від цього вантажу, перетворивши його в

прийнятні для нього форми багатства або доходу. Відповідно, ще одним напрямком діяльності СБ повинне бути вивчення й відстеження змін у способі життя співробітників, що входять у так називані "групи ризику", тобто безпосередні контакти, що мають, із грошовими або матеріальними цінностями, важливою інформацією, що приймає рішення про розподіл і рух цінностей і т.п.

Така діяльність заснована на одержанні, обробці й аналізі інформації про наявних у співробітників й у їхніх родинах матеріальних цінностях, рівні статку й благополуччя, а також на вивченні динаміки зміни до кращого, що співвідносить із показниками легального доходу.

Інформацію таку можна одержати:

А. - від самого співробітника, наприклад при заповненні їм при прийомі на роботу, а також переміщеннях по службі анкет з певними питаннями про наявність у нього основних цінностей (машина, нерухомість й ін.);

Б. - з різних державних джерел - податкових органів, організацій, що реєструють угоди з нерухомістю, ДАІ й ін.;

В. - з реєстраційних і ліцензійних органів про наявність заснованих співробітником або членами його родини фірм, підприємств і т.п.;

Г. - за результатами оперативної роботи;

Д. - шляхом розрахунку основного капіталу.

Застосовується, як правило, відносно особи, у чомусь уже підозрюваного, при використанні наступної формули:

З = А + ОК + ВЖ – (Б+ЗВД)

Засоби з невідомих джерел = Активи (усе, що є) - Основний капітал за попередній період (усе, що було, наприклад, до початку роботи в даній посаді) - Борги + Витрати на життя - Засобу з відомих джерел.

Підсумок Отже, спробуємо підвести якийсь підсумок. Робота СБ по організації протидії шахрайству у всіх випадках починається з одержанням з будь-якого джерела будь-якої інформації, що містить перераховані вище ознаки здійснення, приховання й реалізації викраденого. Але виявити - це не тільки довідатися.

Алгоритм виявлення, як одного з етапів протидії шахрайству, такий:

1. Одержання керівником СБ інформації про (у порядку збільшення складності розробки):

а) факті протиправної дії, що готується; далі тут треба локалізація діяльності СБ на персонах і на території, зазначеної в інформації, для

піймання зловмисників (етап виявлення й розслідування може бути яскраво не виражений);

б) факті, що відбиває наслідку здійснення шахрайства; далі тут випливають дії "від зворотного", тобто від виявлення, наприклад, пропажі цінностей, до розкручування ланцюжка руху цінностей до початку, тобто вже починається розслідування;

в) факті шахрайства, що происшли, по конкретних ознаках здійснення;

г) факті шахрайства, що происшли, по конкретних ознаках приховання;

д) аномальної або підозрілої тенденції, динаміці, явищі в діяльності підприємства;

е) підозрілих змінах у способі життя й поводженні співробітника.

2. Аналітична діяльність по обробці отриманої інформації.

3. Робота з різного роду документами з метою пошуку конкретних ознак здійснення (для 1.г) і/або приховання (для 1.в).

4. Визначення по виявлених ознаках рівня здійснення шахрайства.

5. Систематизування зібраних первинних даних для початку розслідування.

Зрозуміло, у деяких випадках грань між виявленням і проведенням яких-небудь уже слідчих дій по факті шахрайства дуже тонка й зовсім не принципова. Адже в житті розподіл на етапи дуже умовно, головне, - мета й результат.

На закінчення приведемо деякі приклади здійснення шахрайських дій, цього разу при обслуговуванні встаткування й наданні транспортних послуг, а для торговельних компаній - при відвантаженні й доставці товару замовникам. Механізми профілактики й/або виявлення таких дій практично не відрізняються від рекомендованих вище.

Шахрайство при обслуговуванні встаткування

1.) Шахрайство зі строками експлуатації механізмів й устаткування:

- завищення строків для списання з метою присвоєння або реалізації;
- завищення строків для зниження ціни при розпродажі б/у встаткування з метою одержання винагороди від покупця;
- завищення строків для підміни робочого встаткування списаним з метою присвоєння робітника або покупки його в особистих цілях

при розпродажі б/у або присвоєнні коштів , виділених для закупівлі аналогічних механізмів.

2.) Шахрайство з нормами витрати:

- збільшення норм із метою дозакупки "необхідного" кількості матеріалів в особистих цілях або присвоєння коштів , виділених на ці потреби;
- присвоєння видаткових матеріалів, нібито використаних у результаті навмисного, не відповідним реальним умовам, завищення норм.

3.) Використання видаткових матеріалів в особистих цілях.

4.) Шахрайство при технічному обслуговуванні й ремонті встаткування:

- оплата нездійсненого Тоир або завищення оплати;
- змова із представниками обслуговуючих організацій для оформлення фіктивного гарантійного обслуговування або оплати неіснуючого виклику фахівців.

Шахрайство при наданні транспортних послуг

1. Шахрайство при експлуатації свого або орендованого автотранспорту.

а) шахрайство з обліком, тобто з документальним відбиттям певних фізичних або фінансових показників:

- приписки, тобто завищення виконавцями або посадовими особами реальних даних відпрацьованого часу й пробігу;
- завищення строків експлуатації й норм витрати (див. вище),

б) використання транспорту в особистих цілях або з метою наживи,

в) шахрайство при Тоир (див. вище).

2. Шахрайство при користуванні послугами сторонніх транспортних організацій:

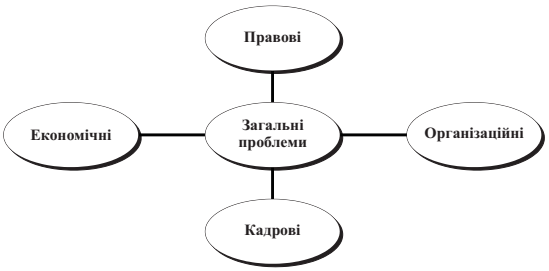
- завищення посадовою особою підприємства в змові із представниками транспортно-експедиційної організації оплати за надавані послуги з метою присвоєння різниці коштів або одержання винагороди;
- організація або установа "своїх" фірм, що надають транспортні послуги, і постійне до них обіг (як правило, разом із завищенням вартості послуг);
- оплата незроблених або повна оплата (зроблених неякісно послуг;

- шахрайство при оплаті оренди транспорту роздільно від оплати витраченого часу використання або витраченого палива;
- шахрайство зі страхуванням вантажів.

4.6. Загальні проблеми діяльності служби безпеки, та шляхи їх вирішення

Аналіз практики функціонування служб безпеки дозволяє затверджувати, що слабка ефективність їхньої діяльності в значній мірі є наслідком існування різних проблем. Всі ці проблеми настільки переплетені один з одним, що розмежування їх між собою на практиці неможливо. Проте автори порахували необхідним зробити це, тому що розмежування цих проблем дозволяє в самому загальному виді сформулювати способи їхнього рішення.

Проблеми ці можна звести в **чотири групи:**



- правові,
- організаційні,
- кадрові
- економічні.

Розглянемо ці проблеми й короткі пропозиції по їхньому рішенню

1. Відсутність типового Статуту служби безпеки. Розробку, твердження й офіційне опублікування типового Статуту служби безпеки можна доручити Міністерству юстиції України.

2. Неефективна взаємодія служб безпеки із правоохоронними й органами, що контрольно-наглядають за ними.

Правила й процедури такої взаємодії для кожного органа окремо в рамках його компетенції можуть бути визначені в спеціальній постанові Уряду України.

3. Заборона на носіння й застосування зброї при охороні життя й здоров'я фізичних осіб. Така безглузда й необґрунтована заборона легко скасувати шляхом внесення відповідних виправлень у чинне законодавство.

4. Відсутність закріпленого в законі переліку основних функцій служби безпеки.

Необхідно у відповідні розділи Законів України внести як виправлення, так і зміни (зазначений перелік цих функцій.)

5. Стримування розвитку служби безпеки у зв'язку з високими податковими відрахуваннями.

У законодавчому порядку встановити перелік податків, зборів і т.д. для служб безпеки й пільгового режиму оподатковування на початку їхньої діяльності (на рік, на три роки т.д.).

6. Внести необхідні виправлення в Закони України для визнання служби безпеки як самостійної комерційної недержавної правоохоронної організації.

7. Заборона про надання службою безпеки підприємства послуг іншим фізичним й юридичним особам. Внести необхідні виправлення в Закони України із застереженням, що такі послуги служба безпеки може здійснювати за згодою керівництва підприємства-засновника та своїх Статутних норм.

8. Відсутність методики визначення необхідної кількості співробітників служби безпеки для даного підприємства. Яка-небудь громадська організація (фонд), що займається проблемами безпеки в сфері підприємництва, могла б оголосити конкурс на розробку такої методики.

9. Сполучення функцій видачі ліцензії, реєстрації й контролю за діяльністю служб безпеки в одному державному органі. Представляється, що видача ліцензій, реєстрація співробітників і самої служби безпеки повинні бути закріплені за органами Міністерства юстиції, функцію же контролю залишити за органами внутрішніх справ.

10. Відсутність у керівників служб безпеки необхідних правових й організаційно-управлінських знань, умінь і навичок. Розробка для цієї категорії керівників силами викладачів недержавних освітніх установ програм спецкурсів.

11. Заборона видачі ліцензій громадянам, що мають судимість за здійснення тільки навмисного злочину та, що мають непогашену судимість і ненавмисні злочини.

12. Відсутність нормативних підстав для однобічного припинення дії договору з підприємством-засновником. Необхідно в законодавчому порядку зафіксувати такі підстави, як протиправні дії керівництва підприємства-засновника, затримки з видачею зарплати, незаконні

вказівки, тому що існуючий у законодавстві порядок розірвання договору не містить ясного й вичерпного переліку таких підстав.

13. Недосконаліть статистичного обліку результатів діяльності служби безпеки. Доцільне створення в органах Міністерства юстиції єдиного й детального обліку результатів діяльності служб безпеки по муніципальних територіальних утвореннях, регіонам і країні в цілому.

14. Залучення колишніх працівників МВС, СБУ та інших категорії законослухняних і професійно грамотних співробітників до роботи в службах безпеки (наприклад, у штабних підрозділах) тільки зміцнить у них стан законності й дисципліни.

15. Неможливість дій співробітників служби безпеки поза державною територією України. Рішення цієї проблеми бачиться в підписанні міждержавних угод, що регламентують порядок дій співробітників служби безпеки на території іншої країни.

16. Необхідність письмової згоди підприємця про висновки їхнього комерційного контракту на з'ясування біографічних й інших характеризующих особистості контрагентних даних. Загально відомо, що на практиці така згода ніколи не дається. Варто внести відповідні корективи в чинне законодавство, тому що підприємницька діяльність в умовах ризику вимагає, серед іншого, інформацію про особистості ділового партнера.

17. Невідповідність між окремо задекларованими у Законах України загальною позицією законодавця про визнання приватних охоронно-детективних структур комерційними організаціями й закріпленням у цих Законах статусу служб безпеки як структурних підрозділів підприємства. Доцільно внести відповідні виправлення про визнання служби безпеки - комерційною організацією, що має право містити договори на обслуговування багатьох підприємств.

Зовсім очевидно, що авторами перерахована тільки частина проблем діяльності служб безпеки підприємств. В попередніх матеріалах були викладені різні шляхи для усунення перешкод в роботі Служби безпеки. Однак сама постановка цих питань дозволяє стверджувати, що рано або пізно вирішувати їх прийде на державному рівні. Авторам залишається тільки сподіватися, що свої міркування, пропозиції, ради й т.д., викладені в дійсній роботі, підштовхнуть уважного й допитливого читача до формулювання інших, (своїх)проблем діяльності служб безпеки й пропозицій по їхньому рішенню. Пропонуємо цю тему для загальної дискусії на семінарських заняттях.

Розділ 5.

Оперативно-розвідувальна діяльність. Контррозвідка. Спостереження.

Програмна анотація

5.1. Менеджмент оперативно-розвідувальної діяльності (ОРД),

– основні поняття оперативно-розвідувальної діяльності підприємницьких структур, і їх відмінність від оперативно-розшукової діяльності державних органів,

– правове регулювання здійснення ділової розвідки в Україні.

5.2. Менеджмент контррозвідувальної діяльності,

– основні характеристики роботи контр розвідувального підрозділу,

– основні методи роботи працівника контр розвідувального підрозділу.

5.3. Спостереження у підприємницькій діяльності,

– ведення зовнішнього спостереження (ЗС),

– виявлення зовнішнього спостереження.

5.1. Менеджмент оперативно-розвідувальної діяльності (ОРД)

Законодавство України допускає збір відомостей про ринок, про надійність і кредитоспро-можність партнерів, про порушення авторських і суміжних прав, про недобросовісну конкуренцію, про розголошування комерційної таємниці і т.д. - громадянами-підприємцями або службами безпеки (СБ) підприємств практично без обмежень. Правовою основою діяльності підрозділу Служби безпеки недержавних об'єктів по збору і аналізу інформації є ст. 34 Конституції України:

Стаття 34. Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей,
для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

На сьогодні правовідносини, що виникають в процесі реалізації права власності на інформацію, яка відноситься до комерційної таємниці, врегульовані, і викладені в цьому розділі в повному переліку, зокрема: Цивільним та Господарським кодексом України, Законом України „Про інформацію", Законом України „Про захист від недобросовісної конкуренції", Законом України „Про науково-технічну інформацію", Постановою Кабінету Міністрів України „Про перелік відомостей, що не становлять комерційної таємниці" від 9 серпня 1993 року № 611 та інше.

Відсутність повноцінного правового регулювання питань, пов'язаних з правом осіб на інформацію, яка відноситься до комерційної таємниці, фактично створює умови для поширення комерційного шпигунства, безперешкодного використання окремими особами незаконно отриманих наукових технологій, програмних продуктів, ноу-хау та іншої інформації або відомостей, які відноситься до комерційної таємниці.

У зв'язку з набранням чинності з 1 січня 2004 року Цивільним і Господарським кодексами України та з огляду на потребу стимулювання роз-

витку підприємницької діяльності виникає необхідність додаткового законодавчого врегулювання сфери інформаційних відносин.

Цивільний кодекс України, визначаючи перелік майнових прав, пов'язаних з правом інтелектуальної власності щодо комерційної таємниці (ст.ст.505-508), не встановлює (оскільки за своїм спрямуванням і не повинен встановлювати) правового режиму комерційної таємниці, порядку віднесення інформації до комерційної таємниці, підстав виникнення прав суб'єктів на комерційну таємницю, порядку доступу до комерційної таємниці тощо.

Згідно з частиною першою статті 36 Господарського кодексу України склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону. Таким чином, вдосконалення правового регулювання відносин щодо визначення, використання, поширення, збереження та захисту комерційної таємниці – прерогатива спеціального закону, який на сьогодні відсутній.

В той же час, згідно з частиною другою статті 505 Цивільного кодексу України, деякі відомості технічного, організаційного, комерційного, виробничого характеру, що не можуть бути віднесені до комерційної таємниці, також визначаються законом. Проте, нині відсутній закон, який визначає, які саме відомості не можуть бути віднесені до комерційної таємниці. Постанова Кабінету Міністрів України від 9 серпня 1993 року № 611 „Про перелік відомостей, що не становлять комерційної таємниці" була прийнята на виконання Закону України „Про підприємства в Україні", який втратив чинність у зв'язку із вступом в силу Господарського кодексу України, що також свідчить про необхідність критичного перегляду зазначеного переліку зважаючи і на те, що він не відповідає існуючим реаліям розвитку конкурентного середовища.

Чинне законодавство не встановлює заходів захисту комерційної таємниці, не визначає конкретний механізм реалізації прав власників комерційної таємниці. Недосконалість чинного законодавства позбавляє власників інформації, яка відноситься до комерційної таємниці, належного захисту своєї власності, обмежує можливість реалізації прав особи щодо інформації з обмеженим доступом, яка створюється в процесі діяльності суб'єктів, завдає матеріальної та нематеріальної шкоди власникам комерційної таємниці.

У зв'язку з цим фактично неможливе застосування норм про притягнення до адміністративної та кримінальної відповідальності за незаконне отримання, використання, збирання та розголошення комерційної таємниці. Так, частиною третьою статті 164-3 Кодексу України про адміністративні правопорушення передбачено адміністративну відповідальність за отримання, використання, розголошення комерційної таємниці з метою заподіяння шкоди діловій репутації або майну іншого підприємця. Кримінальним кодексом України встановлено відповідальність за незаконне збирання з метою використання (комерційне шпигунство) або використання відомостей, що становлять комерційну таємницю (ст.231) та за розголошення комерційної таємниці (ст.232).

Законом України „Про захист від недобросовісної конкуренції" встановлюється відповідальність за неправомірне збирання комерційної таємниці, розголошення комерційної таємниці, її неправомірне використання та за схиляння до розголошення комерційної таємниці (ст.ст.16-19).

Ці правопорушення визнаються за цим Законом недобросовісною конкуренцією.

У Кодексі України про адміністративні правопорушення, Кримінальному кодексі України, Цивільному кодексі України, Господарському кодексі України та у Законі України „Про захист від недобросовісної конкуренції" застосовується поняття „комерційна таємниця". Наявність декількох узагальнюючих законодавчих визначень цього поняття сприяє правопорушникам уникати покарання, а власники комерційної таємниці позбавляються можливості ефективного захисту своїх законних прав та інтересів.

Крім цього, Закон України „Про інформацію" не встановлює чіткого розмежування понять конфіденційної інформації та комерційної таємниці. Відповідно до частини першої статті 30 Закону України „Про інформацію" за режимом доступу інформація поділяється на конфіденційну та таємну. В цьому Законі не встановлено, в чому саме полягає особливість правового режиму інформації комерційного та банківського характеру, але однозначно встановлюється, що такі відомості не можуть бути конфіденційною інформацією.

Зміст поняття «оперативно-розвідувальна діяльність служби безпеки підприємства» та її відмінність від «оперативно-розшукової діяльності» державних органів

Оперативно розвідувальна діяльність (ОРД) служби безпеки підприємства - це діяльність спеціальних підрозділів СБ недержавного підприємства, спрямована на захист своїх законних прав та інтересів від зовнішніх і внутрішніх загроз, недобросовісної конкуренції, своєчасне виявлення і надання керівництву підприємства закритої інформації про реальні і потенційні зовнішні погрози його функціонуванню.

Розвідувальна інформація - це добуті відомості про реальні та потенційні можливості, плани, наміри і дії конкурентів, організацій (в тому числі-злочинних) та окремих осіб, що зачіпають економічні інтереси підприємства, про події і обставини, що стосуються даного підприємства та направлена на своєчасне інформування про методи, способи і осіб, що мають намір (або що виконали цей намір) завдати збитку підприємству і/або його персоналу; а також сприяння правоохоронним, судовим і контрольно-наглядовим органам в притяганні до відповідальності юридичних і фізичних осіб, дії яких зачіпають інтереси підприємства-засновника.

Від **«оперативно-розшукової діяльності»** (ОРД) державних органів, **«оперативно-розвідувальна діяльність»** (ОРД) служби безпеки підприємства відрізняється:

- завданням (пошук, фіксація фактичних даних);
- об'єктом діяльності;
- поняття (система гласних і негласних пошукових, розвідувальних, контр розвідувальних заходів;
- правовою основою діяльності;
- підрозділи, які здійснюють оперативно-розшукової діяльність;
- підстави для здійснення оперативно-розшукової діяльності;
- використання матеріалів оперативно-розшукової діяльності;
- нагляд за оперативно-розшуковою діяльністю;
- таке інше.

Місце і роль оперативно-розвідувальної діяльності в комплексній системі безпеки підприємства.

Питання про місце ОРД в організаційній ієрархії підприємства сильно залежить від вимог, що пред'являються до неї керівництвом.

Але у будь-якому випадку даний підрозділ повинен так побудувати свою роботу, щоб не виявитися поступово відтісненим на підприємстві на

“треті ролі”, подалі від його керівництва. Система збору інформації ефективно працюватиме тільки при постійному контакті із зовнішнім середовищем і з керівництвом підприємства, що ухвалює рішення.

Положення ОРД на конкретному підприємстві визначається рядом чинників: позицією, яку займають власники і керівництво підприємства, їх компетентністю і практичним управлінським досвідом, особистими і діловими інтересами, діловими якостями особового складу підрозділу розвідки.

За оцінкою спеціалістів, українська дійсність дає можливість говорити про те, що найважливішим чинником, що визначає стан системи управління господарюючим суб’єктом (одним з найважливіших компонентів якого є розвідка) є особиста позиція його першого керівника.

Основними чинниками, що формують особисту позицію, є:

- зовнішні чинники (стан ринку, політика держави, дії конкурентів і т.д.);
- особиста позиція (стан здоров’я, рівень агресивності зовнішнього середовища по відношенню до нього особисто, що мають можливості по зміні сфери діяльності і ін.);
- прийнята особиста стратегія (як довго знаходиться на цій посаді, чи розвивати дану організацію в цілому, по окремих напрямах або взагалі готувати до банкрутства, в які сфери вкладати свою енергію і т.п.);
- психологічна готовність і ділові здібності першої особи по організації ефективного оперативного функціонування і стратегічного розвитку підприємства.

Зовсім необов’язково комплектувати підрозділ розвідки повністю ветеранами спецслужб або правоохоронних органів. Як показує практика, достатньо 30% висококласних фахівців (які складуть кістяк підрозділу) для ефективного навчання підростаючого покоління.

Треба відразу обмовитися, що в даному підрозділі немає місця людям, що не мають потреби в засвоєнні нових знань, що не уміють встановлювати контакти, схильним до конфліктної поведінки. Робота по добуванню інформації, не дивлячись на послуги глобальних комп’ютерних мереж, преси і електронних засобів масової інформації, - це, в першу чергу, робота з людьми, а як говорять китайці «людині із злим обличчям не можна відкривати власну лавку», і працювати в розвідці – додають автори.

Додаток: ПРАВОВЕ РЕГУЛЮВАННЯ ЗДІЙСНЕННЯ ДІЛОВОЇ РОЗВІДКИ В УКРАЇНІ

1. **КОНСТИТУЦІЯ УКРАЇНИ.** Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року, (ВВР, 1996, № 30, с.141).

2. **КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ** від 5.04.2001 (ВВР, 2001, №№ 25-26, с.131).

3. **КОДЕКС УКРАЇНИ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ** від 07.12.1984 (ВВР, 1984, додаток до № 51, ст.1122).

4. **МИТНИЙ КОДЕКС УКРАЇНИ** від 11.07.2002 (Відомості Верховної Ради (ВВР), 2002, №№ 38-39, ст.288)

5. **ГОСПОДАРСЬКИЙ КОДЕКС УКРАЇНИ** від 16.01.2003 (Відомості Верховної Ради (ВВР), 2003, №№ 18-22, ст.144)

6. **ЦИВІЛЬНИЙ КОДЕКС УКРАЇНИ** від 16.01.2003 (Відомості Верховної Ради (ВВР), 2003, №№ 40-44, ст.356)

7. **ГОСПОДАРСЬКИЙ ПРОЦЕСУАЛЬНИЙ КОДЕКС УКРАЇНИ** від 06.11.1991 (Відомості Верховної Ради (ВВР), 1992, № 6, ст.56)

8. **КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНИЙ КОДЕКС УКРАЇНИ** (Затверджений Законом від 28.12.60 (1000-05) ВВР, 1961, N 2 ст. 15)

9. ЗАКОН УКРАЇНИ **„ПРО ІНФОРМАЦІЮ"** від 02.10.92, (ВВР, 1992, № 48, с.650).

10. ЗАКОН УКРАЇНИ **„ПРО НАУКОВО-ТЕХНІЧНУ ІНФОРМАЦІЮ"** від 25.06.93, (ВВР, 1993, № 33, с.345)

11. ЗАКОН УКРАЇНИ **„ПРО ДЕРЖАВНУ ТАЄМНИЦЮ"** від 21.01.94, (ВВР, 1994, № 16, с.93). (В редакції Закону № 1079-XIV від 21.09.99).

12. ЗАКОН УКРАЇНИ **„ПРО ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ"** від 05.07.94, (ВВР, 1994, № 31, с.286).

13. ЗАКОН УКРАЇНИ **„ПРО НАУКОВУ І НАУКОВО-ТЕХНІЧНУ ДІЯЛЬНІСТЬ"** від 13.12.91, (ВВР, 1992, № 12, с.165). (В редакції Закону № 284-XIV від 01.12.98).

14. ЗАКОН УКРАЇНИ **„ПРО НАУКОВУ І НАУКОВО-ТЕХНІЧНУ ЕКСПЕРТИЗУ"** від 10.02.95, (ВВР, 1995, № 9, с.56)

15. ЗАКОН УКРАЇНИ **„ПРО ЕКОЛОГІЧНУ ЕКСПЕРТИЗУ”** від 09.02.1995 (Відомості Верховної Ради (ВВР), 1995, № 8, ст.54)

16. ЗАКОН УКРАЇНИ **„ПРО СУДОВУ ЕКСПЕРТИЗУ”** від 25.02.1994 (Відомості Верховної Ради (ВВР), 1994, N 28, ст.232)

17. ЗАКОН УКРАЇНИ **„ПРО КОНЦЕПЦІЮ НАЦІОНАЛЬНОЇ ПРОГРАМИ ІНФОРМАТИЗАЦІЇ”** від 4.02.1998, (ВВР, 1998, № 27-28, с.182).

18. ЗАКОН УКРАЇНИ **„ПРО ДЕРЖАВНУ СТАТИСТИКУ”** від 17.09.1992 (Відомості Верховної Ради (ВВР), 1992, N 43, ст.608)

19. ЗАКОН УКРАЇНИ **„ПРО ТЕЛЕКОМУНІКАЦІЇ”** від 18.12.2003.

20. ЗАКОН УКРАЇНИ **„ПРО ПОШТОВИЙ ЗВ'ЯЗОК”** від 04.10.2001 (Відомості Верховної Ради (ВВР), 2002, № 6, ст.39)

21. ЗАКОН УКРАЇНИ **„ПРО ЛІЦЕНЗУВАННЯ ПЕВНИХ ВИДІВ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ”** від 1.06.2000, (ВВР, 2000, № 36, с.299).

22. ЗАКОН УКРАЇНИ **„ПРО БАНКИ І БАНКІВСЬКУ ДІЯЛЬНІСТЬ”** від 7.12.2000, (ВВР, 2001, № 5-6, с.30).

23. ЗАКОН УКРАЇНИ **„ПРО НАЦІОНАЛЬНУ СИСТЕМУ КОНФІДЕНЦІЙНОГО ЗВ'ЯЗКУ”** від 10.01.2002, (ВВР, 2002, № 15, с.103).

24. ЗАКОН УКРАЇНИ **„ПРО СТАНДАРТИЗАЦІЮ”** від 17.05.2001, (ВВР, 2001, № 31, с. 145)

25. ЗАКОН УКРАЇНИ **„ПРО ОПЕРАТИВНО-РОЗШУКОВУ ДІЯЛЬНІСТЬ”** від 18.02.1992 (Відомості Верховної Ради (ВВР), 1992, № 22, ст.303)

26. ЗАКОН УКРАЇНИ **„ПРО СЛУЖБУ БЕЗПЕКИ УКРАЇНИ”** від 25.03.1992 (Відомості Верховної Ради (ВВР), 1992, № 27, ст.382)

27. ЗАКОН УКРАЇНИ **„ПРО РОЗВІДУВАЛЬНІ ОРГАНИ УКРАЇНИ”** від 22.03.2001 (Відомості Верховної Ради (ВВР), 2001, № 19, ст.94)

28. ЗАКОН УКРАЇНИ **„ПРО АВТОРСЬКЕ ПРАВО І СУМІЖНІ ПРАВА”** від 23.12.1993 (Відомості Верховної Ради (ВВР), 1994, № 13, ст.64)

29. ЗАКОН УКРАЇНИ **„ПРО АНТИМОНОПОЛЬНИЙ КОМІТЕТ УКРАЇНИ”** від 26.11.1993 (Відомості Верховної Ради (ВВР), 1993, № 50, ст.472)

30. ЗАКОН УКРАЇНИ **„ПРО ЗАХИСТ ЕКОНОМІЧНОЇ КОНКУРЕНЦІЇ”** від 11.01.2001 (Відомості Верховної Ради (ВВР), 2001, N 12, ст.64)

31. ЗАКОН УКРАЇНИ **„ПРО ЗАХИСТ ВІД НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ”** від 7.06.1996 (Відомості Верховної Ради (ВВР), 1996, N 36, ст.164)

32. ЗАКОН УКРАЇНИ **„ПРО ЗОВНІШНЬОЕКОНОМІЧНУ ДІЯЛЬНІСТЬ”** від 16.04.1991 (Відомості Верховної Ради (ВВР), 1991, N 29, ст. 377)

33. ЗАКОН УКРАЇНИ **„ПРО АУДИТОРСЬКУ ДІЯЛЬНІСТЬ”** від 22.04.1993 (Відомості Верховної Ради (ВВР), 1993, № 23, ст.243)

34. ЗАКОН УКРАЇНИ **„ПРО БІБЛІОТЕКИ І БІБЛІОТЕЧНУ СПРАВУ”** від 27.01.1995 (Відомості Верховної Ради (ВВР), 1995, № 7, ст.45)

35. ЗАКОН УКРАЇНИ **„ПРО НАЦІОНАЛЬНИЙ АРХІВНИЙ ФОНД ТА АРХІВНІ УСТАНОВИ”** від 24.12.1993 (Відомості Верховної Ради (ВВР), 1994, № 15, ст.86)

36. ЗАКОН УКРАЇНИ **„ПРО ДЕРЖАВНУ СЛУЖБУ”** від 16.12.1993 (Відомості Верховної Ради (ВВР), 1993, № 52, ст.490)

37. ЗАКОН УКРАЇНИ **„ПРО ДЕРЖАВНУ ПОДАТКОВУ СЛУЖБУ В УКРАЇНІ”** від 04.12.1990 (Відомості Верховної Ради (ВВР), 1991, № 6, ст. 37)

38. ЗАКОН УКРАЇНИ **„ПРО РЕКЛАМУ”** від 03.07.1996 (Відомості Верховної Ради (ВВР), 1996, № 39, ст. 181)

39. ЗАКОН УКРАЇНИ **„ПРО ДРУКОВАНІ ЗАСОБИ МАСОВОЇ ІНФОРМАЦІЇ (ПРЕСУ) В УКРАЇНІ”** від 16.11.1992 (Відомості Верховної Ради (ВВР), 1993, № 1, ст. 1)

40. ЗАКОН УКРАЇНИ **„ПРО ПАТЕНТУВАННЯ ДЕЯКИХ ВИДІВ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ”** від 23.03.1996 (Відомості Верховної Ради (ВВР), 1996, № 20, ст. 82)

41. ЗАКОН УКРАЇНИ **„ПРО ТЕЛЕБАЧЕННЯ І РАДІОМОВЛЕННЯ”** від 21.12.1993 (Відомості Верховної Ради (ВВР), 1994, № 10, ст. 43)

42. ЗАКОН УКРАЇНИ **„ПРО НАЦІОНАЛЬНУ РАДУ УКРАЇНИ З ПИТАНЬ ТЕЛЕБАЧЕННЯ І РАДІОМОВЛЕННЯ”** від 23.09.1997 (Відомості Верховної Ради (ВВР), 1997, № 48, ст.296)

43. ЗАКОН УКРАЇНИ **„ПРО СИСТЕМУ СУСПІЛЬНОГО ТЕЛЕБАЧЕННЯ І РАДІОМОВЛЕННЯ УКРАЇНИ”** від 18.07.1997 (Відомості Верховної Ради (ВВР), 1997, № 45, ст.284)

44. ЗАКОН УКРАЇНИ **„ПРО ІНФОРМАЦІЙНІ АГЕНТСТВА”** від 28.02.1995 (Відомості Верховної Ради (ВВР), 1995, № 13, ст. 83)

45. ЗАКОН УКРАЇНИ **„ПРО ПОРЯДОК ВИСВІТЛЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ ТА ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ ЗАСОБАМИ МАСОВОЇ ІНФОРМАЦІЇ”** від 23.09.1997 (Відомості Верховної Ради (ВВР), 1997, № 49, ст.299)

46. ЗАКОН УКРАЇНИ **„ПРО ВИДАВНИЧУ СПРАВУ”** від 05.06.1997 (Відомості Верховної Ради (ВВР), 1997, N 32, ст.206)

47. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ **„Про Положення про технічний захист інформації в Україні”** від 27.09.1999 № 1229/99

48. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ **„Про заходи щодо захисту інформаційних ресурсів держави”** від 10.04.2000 № 582/2000

49. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ **„Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні”** від 31.07.2000 № 928/2000

50. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ **„Про Положення про Державний комітет зв'язку та інформатизації України”** від 03.06.1999 № 601/99

51. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ **„Про Положення про порядок здійснення криптографічного захисту інформації в Україні”** від 22 травня 1998 р. № 505/98

52. ДЕКРЕТ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ **„Про стандартизацію і сертифікацію”** від 10.05.1993 (Відомості Верховної Ради (ВВР), 1993, N 27, ст.289)

53. ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ від 17 листопада 1997 р. № 1287 **„Про державну реєстрацію друкованих засобів масової інформації, інформаційних агентств та розміри реєстраційних зборів”**

54. ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ від 9 серпня 1993 р. № 611 **„Про перелік відомостей, що не становлять комерційної таємниці”**

55. ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ від 27 листопада 1998 р. № 1893 **„Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави”**

56. НАКАЗ ГОЛОВИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 52 від 01.03.2001 **„Про затвердження Зводу відомостей, що становлять державну таємницю”**

57. НАКАЗ ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 61 від 22.12.99 **„Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації”**

58. НАКАЗ ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 35 від 07.06.2002 **„Про затвердження Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації”**

59. НАКАЗ ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 9 від 23.02.2002 **„Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб”**

60. НАКАЗ ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 76 від 24.12.2001 **„Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах”**

61. НАКАЗ ДЕРЖАВНОГО КОМІТЕТУ УКРАЇНИ З ПИТАНЬ РЕГУЛЯРНОЇ ПОЛІТИКИ ТА ПІДПРИЄМНИЦТВА, ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 151/72 від 12.12.2001 **„Про затвердження Порядку контролю за додержанням ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптоси-**

66. НАКАЗ ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 62 від 29.12.1999 **„Про затвердження Положення про державну експертизу в сфері технічного захисту інформації”**

67. НАКАЗ ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ № 53 від 30.11.1999 **„Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації”** № 45 від 22.10.1999 **„Про затвердження Інструкції про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави”**

5.2. Менеджмент контррозвідувальної діяльності

Значення й роль контррозвідки служби безпеки підприємства в сучасних умовах життя обумовлено принаймні двома обставинами:

1) - **по-перше**, прагненням деяких підприємців усунути або нейтралізувати своїх конкурентів за допомогою засобів економічного шпигунства,

2) - **по-друге**, розширенням масштабу криміналізації населення, що створює відповідні умови для його певних шарів вирішувати свої потреби злочинним шляхом. Виходячи із цього, мета контррозвідувального підрозділу можна визначити як протидія розвідувальним заходам конкурентів і припинення правопорушень із боку протиправних груп або окремих осіб, що зазіхали на інтереси підприємства, або його окремих співробітників.

Про призначення контррозвідки точно й коротко висловилася А. Даллес: “Контррозвідка займається в основному захистом й оборонною діяльністю”. На відміну від розвідки, об’єктом контррозвідувальної діяльності є не зовнішня, а внутрішнє середовище функціонування підприємства. Це середовище містить у собі набір певних елементів:

1. Керівний склад підприємства (директор, його заступники, головбух і т.д.) як потенційні об'єкти розвідувальних заходів й/або злочинів з боку конкурентів.

2. Особи з допоміжного персоналу, що мають доступ до комерційної таємниці (друкарки, працівники канцелярії й т.д.).

3. Співробітники, з боку яких потенційно існує небезпека надання злочинним елементам таких відомостей, які допоможуть їм зробити злочину (сторожачи, охоронці, водії персональних машин керівників і т.д.).

4. Співробітники самої служби безпеки.

5. Раніше суджені особи із числа працівників підприємства.

6. Співробітники підприємства, родичі яких працюють у конкурентів.

7. Раніше, що звільнилися з підприємства його працівники.

8. Особи, які в силу своїх посадових обов'язків регулярно приймають відвідувачів підприємства.

А.) **Визначення мети й об'єкта контррозвідувальної діяльності** дозволяє визначити коло можливих завдань підрозділу контррозвідки:

- боротьба з економічним шпигунством;
- припинення злочинів проти окремих груп співробітників (або всіх співробітників на їхніх робочих місцях);
- надання сприяння правоохоронним, судовим і контрольно-наглядовим органам у документуванні протиправних дій осіб, що роблять карні злочини й адміністративні провини.

Б.) Виконання вищевказаних завдань можливо при реалізації наступної сукупності **функцій контррозвідки**:

- збір відомостей і документів по цивільних і кримінальних справах;
- регулярне інформування керівництва підприємства про причини, що породжують й умовах, що сприяють здійсненню правопорушень із боку персоналу;
- документування дій осіб, затриманих за адміністративні провини;
- виявлення осіб із числа персоналу, що роблять сприяння злочинним елементам (не працюючим на підприємстві) у здійсненні ними злочинів;
- викриття економічних (промислових) шпигунів із числа персоналу;
- інформування керівників підприємства й охоронців (якщо вони є) про плановані у відношенні їхніх злочинах;
- пошук без звістки зниклих співробітників підприємства;
- створення умов, що виключають підслуховування розмов у службових кабінетах;
- установлення обставин розголошення відомостей, що становлять комерційну таємницю;
- з'ясування біографічних й інших, що характеризують особистість даних про співробітників підприємства (з їхньої письмової згоди) при висновку ними трудових контрактів;
- пошук втраченого співробітниками майна, що належить підприємству;
- консультування персоналу з питань забезпечення безпеки підприємства.

Характеристики перерахованих вище функцій контррозвідки

Збір відомостей і документів по цивільних і кримінальних справах.

Необхідність у зборі інформації із цивільних справ виникає, звичайно, у випадках:

- виявлення свідків і документів;
- перевірки вірогідності інформації учасників процесу й дійсності доказів, представлених у суді;
- виникнення необхідності перевірки наявності підстави для відводу учасників процесу;

- надання допомоги суду у встановленні фактичного місцезнаходження учасників процесу;
- виявлення осіб, що образили або "оклеветавших" керівників засновника;
- пошуку процесуального супротивника, що приховує від суду майна, необхідного для погашення матеріального збитку;
- необхідності виявлення серед свідків осіб, які в силу своїх фізичних або психічних недоліків не здатні правильно сприймати факти або давати про їх правильні показання й т.д.

Співробітник контррозвідки може займатися збором відомостей як до порушення, так й у процесі судового розгляду цивільної справи. Те ж саме ставиться й до збору відомостей по кримінальних справах. Однак на відміну від цивільної справи керівник контррозвідки зобов'язаний одночасно із цим направити в правоохоронний орган, що робить розслідування, письмове повідомлення. Слід також зазначити, що підрозділ контррозвідки може брати участь у зборі відомостей по всіх цивільних справах підприємства-засновника, у той час як по кримінальних справах, порушеним проти співробітників підприємства тільки із санкції його керівництва.

Регулярне інформування керівництва підприємства про причинах. що породжують й умовах, що сприяють здійсненню правопорушень із боку персоналу. Систематичний аналіз контррозвідувальної інформації дозволяє вчасно і якісно виявляти причини, що породжують й умови, що сприяють здійсненню правопорушень із боку персоналу підприємства. Узагальнені відомості про такий рід причинах й умовах необхідно регулярно представляти керівництву засновника. При цьому важливо не тільки вчасно інформувати про цьому, необхідно також одночасно вносити пропозиції по їхньому усуненню.

Варто також пам'ятати, що перелік причин й умов повинен бути розроблений на рівні підприємства, а не міста, краю, області, країни. Для уточнення такого роду відомостей можливо й проведення анонімного анкетування, однак варто пам'ятати, що його результати напевно будуть перекручені (співробітники підприємства, звичайно, дають правдиві відповіді на багато поставлених питань, крім тих, які зачіпають їхні виробничі інтереси).

Документування дій осіб затриманих за адміністративні провини

Маються на увазі насамперед такі адміністративні правопорушення, які підривають економічну безпеку підприємства (наприклад, дрібні розкрадання) і в силу певних обставин не можуть бути виявлені охоронцями. Протиправні дії адміністративних правопорушників ретельно документуються (довідки, пояснення, акти й т.д.) і передаються в той орган, у компетенцію якого входить їхній розгляд. Особлива увага при цьому варто звернути на те, щоб при затримці правопорушника були присутні очевидці, чия об'єктивність не піддається сумніву (наприклад, не рекомендується запрошувати як очевидець співробітника Служби безпеки.

Виявлення осіб із числа персоналу, що роблять сприяння злочинним елементам (не працюючим на підприємстві) у здійсненні ними злочинів. Оскільки злочинці при реалізації своїх задумів намагаються залучити до негласного співробітництва працівників підприємства, то для цієї категорії персоналу з боку контррозвідки повинне бути приділена найпильніша увага. Із цією метою складається список потенційних помічників злочинцям, і з ними проводиться робота із застосуванням законних методів. Результатом такої роботи повинне бути або документування злочинних дій співробітника підприємства, або відмінювання його до відмови від здійснення злочину.

Викриття економічних (промислових) шпигунів із числа персоналу

Установлення й викриття економічних шпигунів, тобто осіб, що використають незаконні методи, які приводять до матеріального збитку підприємства, є найважливішою функцією контррозвідки. При цьому контррозвідники зобов'язані використати тільки законні методи й засоби. Особлива увага варто приділяти документуванню діяльності шпигунів, що дозволить згодом залучити їх до цивільно-правового, а в деяких випадках і до кримінальної відповідальності.

Інформування керівників підприємства й охоронців (якщо вони є) про виявлені порушення у відношенні їхніх дій.

У процесі контррозвідувальної діяльності треба особлива увага приділяти інформації, що свідчить про підготовку замаху на керівника підприємства. Контррозвідувальне забезпечення в цьому випадку повинне бути сконцентроване в наступних зонах:

а) - квартири сусідів охоронюваної особи;

б) - під'їзд будинку, де проживає охоронюваний;

в) - маршрут пересування;

г) -найбільш відвідувані місця роботи й відпочинку.

Отримана інформація про підготовку замаху на керівника підприємства повинна бути негайно передана начальникові підрозділу охоронців й охоронюваній особі без вказівки джерела інформації.

Пошук без звістки зниклих співробітників підприємства

Без звістки зниклим вважається співробітник підприємства, місцезнаходження й доля якого залишаються невідомими. Пошук припускає широкий із правил (процедур) по встановленню місцезнаходження особистості й не зв'язаний юридично обов'язковими прийомами й засобами розшуку. Діяльність співробітника контррозвідки по розшуку без звістки зниклої особи представляє комплекс самостійних дій, здійснюваних при тісній взаємодії з органами внутрішніх справ для встановлення фактичних обставин його зникнення й фактичного місцезнаходження.

Створення умов, що виключають підслуховування розмов у службових кабінетах. Реалізація цієї функції має виняткове значення, оскільки дозволяє керівництву охоронюваного підприємства зберегти не тільки комерційну таємницю, але й будь-яку конфіденційну інформацію службового характеру. Створити умови, що виключають підслуховування розмов, можна за допомогою організаційних і технічних заходів.

В організаційну групу заходів входять інструктажі, розробка пам'яток і т.д. Технічні заходи містять у собі систематичні обстеження службових приміщень із метою виявлення пристроїв, що підслухують. Особлива увага варто звернути на створення умов, що виключають підслуховування, при проведенні переговорів з діловими партнерами.

Установлення обставин розголошення відомостей, що становлять комерційну таємницю

Комерційною таємницею стає тільки та інформація, що затверджена керівництвом підприємства в "Переліку відомостей, що становлять комерційну таємницю підприємства" й оголошена під розписку всім причетним до неї співробітникам. Під розголошенням комерційної таємниці розуміється навмисна або ненавмисна передача (усно або письмово), без згоди власника (власника) або керівника, визнаних у встановленому порядку такий, стороннім особам або невизначеному колу осіб. Установлення обставин розголошення відомостей, що становлять комерційну таємницю, припускає, що співробітник контррозвідки у зв'язку із цим повинен:

а) - визначити обсяг розголошених відомостей;

б) - установити особу, із чиєї вини ці відомості стали відомі іншим особам;

г) - становити фізичну або юридичну особу, якій були передані цей відомості;

д) - задокументувати всю отриману їм вищевказану інформацію. Передача документів, що підтверджують розголошення комерційної таємниці, у правоохоронний орган відбувається тільки із санкції керівництва підприємства, що обслуговує.

З'ясування біографічних й інших даних, що характеризують особистість, про співробітників підприємства (з їхньої письмової згоди) при висновки виконання ними трудових контрактів.

Зміст інформації про особистості співробітника містить у собі дві групи відомостей:

1) - службові (прогули, скарги відвідувачів і т.д.)

2) - особисті (аморальне поводження, сімейні проблеми й т.д.).

Представляється, що сукупність вищевказаних відомостей може в достатньому ступені охарактеризувати співробітника підприємства й допомогти його керівництву в зміцненні дисципліни. Треба при цьому відзначити, що у випадку звільнення такого співробітника негласні матеріали контррозвідки повинні бути реалізовані у встановленому законом порядку. Однак, перш ніж приступитися до перевірки співробітника, варто переконатися, що він раніше давав письмову згоду на ці дії.

Пошук втраченого співробітниками майна, що належить підприємству

Під втраченим майном розуміється річ, загублена внаслідок недбалості персоналу підприємства. При цьому не має значення, де загублене річ (на території або поза територією охоронюваного об'єкта). Щоб уникнути непорозумінь варто переконатися в наявності документів, що підтверджують володіння цим майном на законних підставах. У випадку позитивного результату пошуку втрачене майно повертається власникові в цивільно-правовому порядку. Якщо в ході пошуку встановлені ознаки злочину, то зібрані матеріали необхідно направити у відповідний правоохоронний орган для рішення питання про порушення кримінальної справи.

Консультування з питань забезпечення безпеки підприємства і його персоналу. Консультування співробітників підприємства відбувається пе-

реважно по всіх видах безпеки. Форми консультування групові (лекції, семінари й т.д.) і індивідуальні. Серед персоналу підприємства варто виділити ті групи, які необхідно систематично інструктувати. Якщо є необхідність, то можна створити спеціалізовані навчальні курси зі здачею заліків. Мети, завдання, функції й інші основні питання діяльності контррозвідки, звичайно, відбиваються в положеннях про контррозвідувальні підрозділи.

На основі затверджених керівництвом служби безпеки й підприємства цілей, завдань і функцій контррозвідки можливе формування її оргструктури. У структурі контррозвідки, на наш погляд, повинні функціонувати наступні підрозділи: власної безпеки, проведення розслідувань, по роботі з інформаторами, довідково-інформаційний фонд (СИФ), попередження правопорушень, по технічному забезпеченню проведення операцій, по організації збереження комерційної таємниці, негласного проникнення, організації дезинформаційних заходів, комп'ютерної безпеки.

Підрозділ (відділення, групи, сектори) контррозвідки умовно можна розділити на дві групи:

а) основні, які властиво й вирішують завдання, поставлені перед контррозвідкою (проведення розслідувань, робота з інформаторами й т.д.);

б) допоміжні, основними завданнями яких є всіляке сприяння співробітникам основної групи (СИФ, технічне забезпечення проведення операцій і т.д.)

Кількісне співвідношення між співробітниками допоміжних й основних відділень (груп, секторів) контррозвідки може бути різним, однак при цьому дві умови повинні бути дотримані обов'язково: співробітники допоміжних підрозділів надають допомогу співробітникам основних підрозділів (а не навпаки); робота співробітників основних підрозділів повинна бути ефективної.

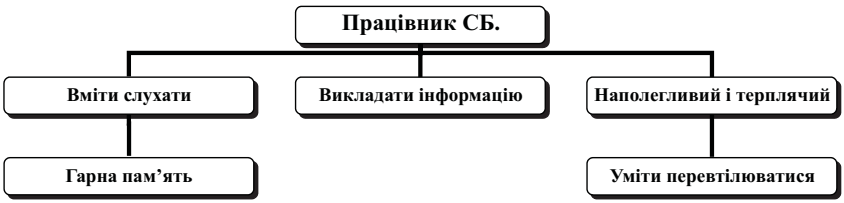
Більше чітке подання про розмежування структурних підрозділів контррозвідки між собою можливо на основі таких параметрів, як надане завдання й форми подання результатів роботи .

Відомо, що комплекс сил, засобів контррозвідки й застосовуваних нею методів у величезному ступені - визначає потенціал контррозвідувальної діяльності. Правда, умовою реалізації цього потенціалу є

активна організаційно-управлінська діяльність керівництва СБ, однак своєрідним базисом такої діяльності є все-таки вищезгаданий комплекс сил, засобів і методів.

До сил контррозвідки відносяться її кадрові співробітники, при цьому вони підрозділяються на тих, які мають ліцензію на детективну діяльність і не мають її (друкарки, водії, секретарі й т.д.). Детективи контррозвідки, крім загальних вимог до співробітників СБ, повинні відповідати наступним вимогам:

- уміти вислухувати співрозмовника,
- ясно й дохідливо викладати в документах інформацію,
- бути наполегливим і терплячими в досягненні мети,
- мати гарну пам'ять,
- уміти перевтілюватися й т.д.



Серед засобів контррозвідувальної діяльності найбільша увага варто приділити фінансовим. Направляти їх треба (крім оплати праці детективів і технічного їхнього забезпечення), у першу чергу, на заохочення праці інформаторів, проведення операцій, транспортні витрати й т.д.

Серед правових засобів до числа обов'язкових, без чого неможливе існування в принципі підрозділу контррозвідки, варто віднести положення про сектор (групі) контррозвідки, посадові інструкції й положення про режим. До матеріально-технічних засобів відносять звичайно автомобілі, радіотелефони, магнітофони, диктофони й т.д. Відносно технічних засобів варто мати на увазі, що їхнє використання обмежене законодавчими нормами.

Інформаційні засоби займають, з деякими застереженнями, центральне місце в системі засобів контррозвідки. Таке положення є закономірним, якщо визначити, що продуктом контррозвідувальної діяльності є знання про об'єкт, що цікавить, причому не всякі, а нові знання.

До числа інформаційних засобів ставляться різні обліки, що допомагають детективам контррозвідки в їхній роботі (причому не завжди доцільно вводити їх у комп'ютерні системи).

Основні методи роботи працівника контррозвідувального підрозділу.

Серед методів, найбільше часто використовуваних співробітниками контррозвідки, можна відзначити наступні:

- ✸ сховане спостереження;
- ✸ відкрите й зашифроване опитування;
- ✸ наведення довідок;
- ✸ вивчення предметів і документів;
- ✸ зовнішній і внутрішній огляд будов, приміщень й ін. об'єктів.

Охарактеризуємо кожний з перерахованих вище методів окремо:

1.) Сховане спостереження - метод негласного, закритого від сторонніх осіб, збору інформації, заснований на візуальному й слуховому сприйнятті з й явищ, а також прийомів їхньої реєстрації, що стосуються досліджуваного об'єкта, значимого з погляду контррозвідувальної діяльності. У процесі такої діяльності застосовується як фізичне, так й електронне спостереження. Згода спостережуваного на використання цього методу не потрібно, однак детективові варто мати на увазі, що застосування його обмежене законодавчими нормами. Наприклад, детектив може без дозволу вести спостереження за співробітником підприємства на його території, однак вести таке спостереження за допомогою електронних засобів у квартирі цього співробітника законом забороняється.

2.) Відкрите й зашифроване опитування - усна бесіда співробітника контррозвідки із заздалегідь наміченою й досліджуваною особою з метою збору фактичних даних про досліджувану подію або причетним до нього особою. Закон не жадає від детектива, щоб він у кожному випадку представлявся, у зв'язку із чим усне опитування може бути зашифрований. Усна згода на проведення бесіди зі співробітником підприємства не потрібно (якщо він при надходженні на роботу давав письмову згоду про застосування стосовно нього методів, зафіксованих у Законі про приватну детективну й охоронну діяльність), однак стосовно інших громадян така згода обов'язково. За результатами опитування можлива (за згодою опитуваного) і фіксація самим опитуваним отриманих відомостей у письмовому виді, записаних на відеомагнітофон і т.п.

3.) Під наведенням довідок розуміється усне або письмове звертання до громадянина із проханням про надання відомостей, що цікавлять детектива, і їхнє одержання (у т.ч. у формі документів). Слід зазначити, що надання такого роду відомостей для співробітників підприємства є обов'язком, для посадових осіб - обов'язком тільки у випадках, коли це встановлено правовими актами, а для інших громадян взагалі є правом, а не обов'язком.

4.) Вивчення предметів і документів означає ознайомлення, всебічне дослідження їх з метою одержання шуканої (необхідної) інформації. Відносно предметів і документів, що належать підприємству, потрібне письмова згода його власника, зафіксоване при установі СБ у його уставі. Що стосується інших предметів і документів, то у відношенні їх потрібно попередня письмова згода їхніх власників. Правда, і в цьому випадку є виключення (наприклад, у відношенні опублікованих правових актів). Крім того, якщо приватному детективові будуть надані будь-якою особою копії предметів і документів (макети, моделі й т.д.), а не оригінали, то згоди власників (власників) не потрібно. Для вивчення предметів і документів (як оригіналів, так й їхніх копій) співробітник контррозвідки вправі залучити експертів, консультантів і т.д.

5.) Зовнішній і внутрішній огляд будов, приміщень й ін. об'єктів означає всебічне візуальне (гласне й/або негласне) їхнє обстеження й вивчення для фіксації необхідних контррозвідникові відомостей. Згода власника на зовнішній огляд законом не передбачено, що стосується внутрішнього огляду об'єктів підприємства, то така згода повинне бути зафіксоване в уставі СБ. При огляді допускається використання технічних засобів і фахівців.

Всі перераховані вище методи можна ефективно застосовувати як роздільно, так і взаємно доповнюючи один одного. Однак найбільш ефективним методом варто визнати все-таки опитування, тому що саме в рамках цього методу можлива діяльність інформаторів.

Інформаторів контррозвідувального підрозділу можна умовно розділити на кілька груп:

1. Працівники підприємства, що інформують про роботу потенційних джерел витоку інформації в силу свого службового становища (наприклад, секретарі, водії персональних машин і т.д.).

2. Сусіди, знайомі, друзі, коханки й т.д., що інформують про правопорушення, що готуються, відносно охоронюваних співробітників підприємства в позаслужбовий час.

3. Особи, що не працюють на підприємстві, але близькі контакти, що мають, зі співробітниками охоронюваного підприємства, які, у свою чергу, є потенційними об'єктами розробки з боку конкурентів.

4. Співробітники контррозвідувального підрозділу служби безпеки, що негласно впровадилися на певний час як співробітник охоронюваного підприємства.

Можлива й інша класифікація методів контррозвідувальної діяльності. Наприклад, у рамках тріади "людина - документ - виріб (процес)" методи одержання контррозвідувальної інформації підрозділяються по такій підставі, як джерела інформації по різним напрямкам.

Для об'єктивної оцінки діяльності контррозвідки необхідно розробити відповідні критерії й показники її діяльності.

Критерії діяльності контррозвідувального підрозділу:

а) - ступінь протидії розвідувальним заходам ділових конкурентів і злочинців,

б) - рівень відвернених і припинених правопорушень на охоронюваному об'єкті.

Показниками, що розкривають вищевказані критерії, можуть бути:

1) кількість притягнутих до відповідальності за розголошення комерційної таємниці підприємства;

2) кількість виявлених економічних (промислових) шпигунів;

3) кількість реалізованих інформаційних матеріалів про причини, що породжують й умов, що сприяють здійсненню правопорушень;

4) кількість вигранних судових процесів по цивільних справах на підставі матеріалів контррозвідки;

5) кількість вигранних судових процесів по кримінальних справах на підставі матеріалів контррозвідки;

6) кількість розглянутих матеріалів, підготовлених контррозвідкою, по адміністративних правопорушеннях;

7) кількість службових розслідувань, проведених відносно персоналу підприємства;

8) кількість розшуканих без звістки зниклих співробітників підприємства;

9) кількість перевірок співробітників підприємства;

10) кількість повернутого підприємству втраченого його співробітниками майна.

5.3. Спостереження

Зовнішнє спостереження — найстародавніший спосіб пізнання світу. З незапам'ятних часів з його допомогою чоловік вивчав місцевість, що оточувала його, розташовані на ній об'єкти і предмети, відзначав зміни, що відбувалися там, і на основі своїх спостережень робив якісь дії.

Зовнішнє спостереження (ЗС) — один із способів ведення детективної діяльності, що має на увазі постійне або вибіркове дослідження стану і діяльності об'єкту спостереження – людину, умовно назвемо «ВІН», (під ВІН надалі ми розумітимемо спостережувану людину, предмет або явище), з подальшим узагальненням і аналізом отриманих в результаті спостереження - даних.

Завдання на спостереження, вирішувані в результаті проведення заходів щодо ЗС можуть бути різні: визначення круга спілкування спостережуваної особи, виявлення його схильностей і інтересів, встановлення розмірів і джерел отримуваних доходів, вивчення графіка роботи, маршрутів руху, системи охорони і ступеня професіоналізму її співробітників, реєстрація різних явищ (діянь, подій, фактів і процесів).

ЗС може вестися візуально або із застосуванням оптичних приладів і технічних засобів. Інтенсивність ЗС залежно від поставлених завдань може бути різною: разове, вибіркове, періодичне, профілактичне і постійне. ЗС може вестися "скритно" (для отримання інформації про об'єкт спостереження) і демонстративно (з метою надання негативної дії на емоційний стан об'єкту). ЗС здійснюється за нерухомими (стаціонарними) і рухомими об'єктами, в останньому випадку ЗС може бути переслідуючим (тобто рухатися услід за ОС) і стрічним (з постів спостереження заздалегідь виставлених в зручних для спостереження точках маршруту ОС). При великому видаленні або при неможливості наближення до ОС для організації ЗС використовуються спеціальні технічні, засоби.

Хотілося б акцентувати Вашу увагу на тому факті, що сучасна організована злочинність приймає на озброєння найсучасніші спеціальні ме-

тоди і засоби. Ні для кого вже не секрет, що достатньо часто злочинців консультують ті, що були, а то і співробітники правоохоронних органів, що володіють веденням оперативно-розшукової діяльності, що відмінно знають методику. І в цьому випадку "дичина" сама стає "мисливцем".

Не маючи в своєму розпорядженні документальних матеріалів що трапилось можна припустити, що виявлення зовнішнього спостереження, що ведеться, стало можливим з кількох причин:

1. Проведення злочинцями заходів щодо контрспостереження, що виражалися в патрулюванні зони контакту, чисельна перевага і раніше виявлення силового прикриття з подальшими одночасними і скоординованими діями з нейтралізації чинника загрози.

2. Швидше за все співробітниками міліції для контролю розмови об'єкту із злочинцями використовувалася звичайна не кварцована радіозакладка, що елементарно виявляється стандартним скануючим приймачем AR-3000, вартістю в різній комплектації від 1000 до 1500 доларів.

3. Недостатнім маскуванням і кваліфікацією співробітників ведучих зовнішнє спостереження.

4. Нечисленністю групи прикриття і розміщення її тільки в одному місці, тобто одночасно прикриваючи і виведений на контакт об'єкт і власного колегу.

Одним з найважливіших завдань зовнішнього спостереження (ЗС), є встановлення зв'язків з об'єктом спостереження (ОС) . При вступі об'єкту до контакту спочатку запам'ятовується зовнішність, костюм контактера, оцінюється характер зустрічі (випадковий, по попередній домовленості, службовий, особистий і т.д.), виявляється ініціатор зустрічі, визначається предмет і тривалість розмови — все це деталлю описується в звіті про виконану роботу.

Особа зв'язків об'єкту ЗС встановлюється за місцем проживання і за місцем роботи. Зазвичай ці заходи проводять один або двоє детективів, що діють під прикриттям комунально-ремонтних служб, співробітників пенсійних фондів, комерційних агентів або групи соціологічного опиту. Інформація збирається у сусідів по сходовому майданчику і по гаражу, у жінок пенсійного віку — біля під'їзду будинку, колег по роботі, працівників комунальних служб і КРЕПів.

Легендування заходів щодо ЗС під дії державних правоохоронних органів і спецслужб **категорично забороняється**. Процес спостереження

дуже складний, оскільки вимагає значних витрат сил і засобів. ЗС, як правило, ведеться цілеспрямовано, "скритно", в потрібному місці, в певний час, спеціально підготовленими для цього людьми.

Слід пам'ятати, що ЗС — робота творча, в ній рідко вдається отримати відповідь на поставлене питання, проводячи операцію за шаблоном, навіть ретельно спланована операція не завжди точно проходить по первинному плану.

Ведення зовнішнього спостереження (ЗС).
(Детектив і бригада зовнішнього спостереження.
Екіпіровка. Способи маскування.)

ЗС може вестися як окремим детективом, так і групою з декількох чоловік. Групу детективів, спільно провідних заходи щодо ЗС ми умовно називатимемо **бригадою ЗС**.

Бригада ЗС зазвичай складається з трьох-чотирьох чоловік і закріпленої за ними автомашини. Бажано, щоб у кожного члена бригади були права водіїв і навики водіння автотранспортного засобу. Це корисно у багатьох випадках: по-перше, розширює оперативні можливості, оскільки дозволяє здійснювати спостереження силами всієї бригади, позмінно підміняючи водія, по-друге, страхує від різних випадковостей — від мухи, що потрапила в очі, до раптового нападу апендициту.

При виявленні об'єкту візуально познайомитися з ним повинні всі члени бригади ЗС, у тому числі і водій.

При жорстких обмеженнях в засобах можливе використання пари детективів, оснащених автотранспортним засобом. Робота поодинці чревата швидкою розшифровкою об'єктом або його оточенням що ведеться за ними ЗС, проте, коли іншого виходу немає — треба задовольнятися доступним. Як вже було сказано вище, найважливішим завданням при веденні ЗС є недопущення розшифровки детектива. Детектив не повинен привертати увагу людей, що оточують його, тому цього одяг повинен бути таким, що не впадає в очі і не привертає погляди перехожих.
Використовуваний гардероб повинен регулярно мінятися, особливо верхня його частина — піджаки, плащі, куртки, головні убори. Детектив в обов'язковому порядку повинен мати в своєму розпорядженні запас одягу, різного по фасону і кольору. Як платтяну шафу можна використовувати автомашину, заздалегідь зробивши заходи по маскуванню одягу, що зберігається в ній. Категорично забороняється зберігати одночасно декілька головних уборів біля заднього скла, особливо коли в машині постійно знаходиться тільки одна людина.

Хорошим маскуванням є використання в ЗС жінок, як поодинці, так і в парі з чоловіком. У цих випадках бригада ЗС працює під «легендою» — «сімейна пара» або «закохані».

Для проведення заходів щодо ЗС детектив повинен бути відповідним чином екіпірований. Ведення ЗС — процес достатньо розтягнутий за часом і чреватий різними поворотами подій. У зв'язку з цим треба заздалегідь поклопотатися про наявність пищи і напоїв, засобів першої медичної допомоги, прав водіїв, посвідчення особи, схеми місцевості, авторучки, блокнота для записів, запасних фотоплівок, відеокасет, грошових коштів, засобів зв'язку і запасних батарей.

Іноді в процесі ведення ЗС буває достатньо складно покинути автомашину з міркувань маскування для облямовування природних потреб, на такий випадок бажано мати судину з широким горлом і кришкою, що щільно закривається.

Оскільки в процесі спостереження за об'єктом можливі декілька пересадок з одного виду транспорту на інший, детектив повинен мати в своєму розпорядженні єдиний проїзний квиток на всі види транспорту і деяку суму готівки дрібними купюрами. Крім цього бажано мати резервну крупну суму на непередбачені витрати, наприклад, для «сумісного» з об'єктом відвідин ресторану або супроводу його в потягу і літаку.

Хоча значна частина роботи може проходити в автомашині, детективові, ведучому ЗС, багато доводиться «топати» пішки в будь-яку погоду. Тому використовуване взуття повинне бути добротним, міцним і зручним. У жодному випадку недопустимий вихід на завдання щодо ЗС в новому не розношеному взутті. Для ведення спостереження використовуються люди з типовими для даної місцевості особами, що не запам'ятовуються, що не мають характерних для пізнання прийме: шрамів, бородавок або родимок. Для якісного ведення ЗС необхідна відмінна пам'ять, залізне терпіння, хороший слух, повноцінний зір, миттєва реакція, уміння імпровізувати і орієнтуватися в будь-якій ситуації, включаючи критичну.

Вік від 25 до 50 років найбільш ефективний, оскільки люди молодшого віку не мають достатнього життєвого досвіду і можуть зробити непродумані дії, що ведуть до розшифровки ЗС перед об'єктом. Люди старше 50 втрачають швидкість реакції, мають проблеми із здоров'ям і довше можуть освоювати нову оперативну техніку.

Детектив, ведучий ЗС, повинен володіти міцним здоров'ям, так як проведення подібних заходів має на увазі багатогодинне знаходження на відкритому повітрі за любої погоди.

Найважливішим правилом ведення ЗС є негайне припинення спостереження при його розшифровці ОС або його оточенням.

Постановка завдання перед бригадою зовнішнього спостереження

Безпосередньо перед проведенням заходу щодо ЗС старший бригади ЗС зобов'язаний провести 10—15-хвилинний інструктаж. Протягом цього часу він повинен чітко і ясно пояснити локальну мету проведення операції (наприклад, узяти об'єкт під спостереження при відході з роботи і супроводжувати його до місця мешкання). Стратегічні цілі проведення операції, тобто яка її спрямованість і для чого необхідна інформаційна фактура, бригаді спостереження знати протипоказано із-за можливого просочування інформації.

Далі, старший повинен поставити завдання перед кожним членом бригади, довести порядок взаємодії і дій в критичних ситуаціях, вказати на минулі недоліки в роботі і сформулювати заходи по їх недопущенню. Також старший обумовлює режим радіо- і візуального зв'язку між членами бригади ЗС. Старший бригади ЗС обов'язково повинен уточнити графік ЗС — пост цілодобового спостереження може бути трьох або чотирьохзмінний. Найбільш оптимальний — 6-годинний режим роботи.

Члени бригади ЗС повинні бути ознайомлені із словесним портретом і фотографією (якщо її не має, то необхідно в процесі ЗС непомітно з різних напрямів сфотографувати об'єкт), описом зовнішності і звичок спостережуваного.

Закінчується інструктаж узгодженням часу і місця збору бригади ЗС, а також способу доставки оперативної техніки і людей до місця проведення заходів щодо ЗС.

Види зовнішнього спостереження

Спостереження із стаціонарних позицій використовується для контролю певної місцевості, окремих будівель, організацій, підприємств, предметів або осіб, що не знаходяться в русі.

1.) Стандартні завдання спостереження із стаціонарних позицій:

- виявлення відвідувачів будівлі, що цікавить, або споруди;
- перехопити розшукувану людину;

- провести “розробку” даної будівлі або споруди для проведення конкретної операції.

2.) **На попередньому етапі** організації НН із стаціонарних позицій необхідно з’ясувати:

- всі можливі шляхи підходу об’єкту НН до місця спостереження зокрема скритні і мало використовувані;
- можливі перспективні шляхи відходу об’єкту з-під спостереження і місця його можливої появи або скритного знаходження;
- часовий розпорядок мешканців будівлі (якщо це житловий будинок) або графік роботи співробітників (якщо це службове приміщення);
- графік руху транспорту, що проходить поряд, і місце його паркування;
- час регулярних звукових сигналів (заводські гудки, шум потягу, що проходить, дзвін церковних дзвонів і т.д.);
- внутрішнє планування довколишніх будівель і споруд.

3.) Внутрішнє планування довколишніх будівель і споруд можна з’ясувати наступними шляхами:

- заглядаючи у вікна і двері;
- проникаючи в місце, що цікавить, під виглядом відвідувача, обслуговуючого персоналу, співробітника ремонтних служб (маючи в наявності відповідні документи прикриття);
- можливе орієнтування по раніше обстежених однотипних будівлях і спорудах, заздалегідь в обов’язковому порядку виявляються всі відхилення від стандартного типового проекту;
- шляхом вивчення креслень з архівів місцевого БТІ або муніципального архітектурного відділу (управління);
- шляхом опиту жителів, обслуговуючого персоналу, будівельників, відвідувачів і т.д.

Для отримання якісніших результатів в процесі проведення ЗС здійснюється обов’язкова реєстрація в журналі спостережень всього спостерігача, що відбувається в зоні відповідальності, а при необхідності — фотографування або зйомка на відео.

Пости стаціонарного спостереження повинні розташовуватися в місцях, де їх тривале перебування з’ясовне і одночасно є можливість контролювати всі підходи до об’єкту. Це можуть бути: стоянки автомашин,

кафе, ресторани, магазини, зняті на підставних осіб квартири, газетні і продуктові намети, зупинки міського транспорту, офіси фірм і т.д.

Спостереження може вестися однією людиною, а якщо можливості по спостереженню значно обмежені, то повинна використовуватися бригада ЗС з 3—4-х співробітників. Оскільки тривале знаходження детективів може викликати підозри, через деякий час їх повинні міняти колеги, що знаходяться поблизу (але поза зоною видимості ВІН), по спостереженню. ЯКЩО скритне розташування спостерігачів пов'язане з певними труднощами, то слід удатися до спостереження з автомобіля (причому в автомашині повинен знаходитися тільки одна людина) або до імітації його поломки подальшим його ремонтом.

При спостереженні з приміщення, рекомендується завісити вікна легеням завісками і вести ЗС з глибини кімнати. Щоб не виявити себе різкими демаскуючими відблисками використовуваної оптики, необхідно використовувати так звані «світлові тунелі».

Супровід об'єкту спостереження при русі пішим порядком

При рухомому спостереженні зазвичай використовуються чотири—шість чоловік або 1—2 бригади спостереження. НС ведеться з таким розрахунком, щоб в безпосередній близькості від об'єкту завжди знаходився лише один спостерігач.

Окрім виконання своїх безпосередніх завдань по утриманню об'єкту в зоні візуального контакту, в його обов'язки входить інформування бригади ЗС про положення ОС. Зв'язок з бригадою здійснюється за допомогою жестів, положення тіла, рук, дій і радіозв'язку. Використання засобів радіозв'язку повинне відбуватися якомога скритніше. Кошти зв'язку повинні бути переказані в режим вібрації (тобто тональний режим), використання звукових сигналів виклику повинне бути, в міру можливості, скорочено.

Знаки, використовувані при ЗС у вигляді коду, як приклад можуть виглядати так:

- "об'єкт стоїть" - руки перехрещені за спиною;
- "об'єкт повернув наліво" - ліва рука упирається в ліве стегно;
- "об'єкт повернув направо" - права рука упирається в праве стегно;
- "об'єкт перетинає вулицю" - півоберт убік із згинанням однієї руки у грудей;

- “об’єкт розвернувся і йде у зворотному напрямі” - одна рука підноситься до голови;
- “об’єкт вийшов з-під контролю” - обидві руки піднімаються до голови;
- “мене треба змінити” - пильний погляд на годинник з імітацією здивування.

Детективові, ведучому ЗС за особою, що є об’єктом спостереження, на першому етапі необхідно з’ясувати місце мешкання об’єкту і його розпорядок дня. Поведінка об’єкту, його контакти, номери використовуваних автомобілів, їх маршрут, розклад потягів і т.д. краще всього надиктовувати на диктофон, а потім розшифровувати і зафіксувати на електронних або паперових носіях.

Позиція, вибрана для спостереження за будинком мешкання об’єкту, повинна бути, по можливості, закрита, тобто не кидатися йому в очі. Для цього підійдуть сквери, під’їзди будинків, будівлі установ і організацій (особливо з безліччю відвідувачів). Особливо зручні вуличні кафе, де, всівшись біля вікна або вибравши столик на вулиці, можна спокійно чекати появи об’єкту спостереження.

Якщо детективи діють в парі, то в очікуванні виходу ОС, необхідно розміститися таким чином: один детектив мається в своєму розпорядженні лицем до місця виходу об’єкту, а інший — спиною. Можлива імітація ділової бесіди. Така позиція дозволяє одному детективу небагато розслабитися і відпочити, тоді як другий-веде спостереження.

Якщо поблизу неможливо сидіти або стояти, не привертаючи до себе уваги, то один з детективів може пересуватися біля місця знаходження ОС, зупиняючись по дорозі під різними приводами: розглядаючи вітрини, розмовляючи з продавцями і т.д. У разі, коли і це по якихось причинах неможливо, то треба зайняти позиції в обох кінцях вулиці і брати об’єкт під спостереження при його русі в одну із сторін.

При появі об’єкту в зоні спостереження необхідно триматися спокійно і урівноважено, у жодному випадку недопустимі різкі рухи. Якщо ОС при виході не відмітив ведучого спостереження детектива, то останньому доцільніше постаратися якось сховатися. Якщо ж він потрапив у поле зору об’єкту, то краще не змінювати положення (якщо ви стоїте) або темпу і напряму руху (якщо ви рухаєтеся) і передати об’єкт іншому детективу. Переслідування об’єкту слід починати тільки тоді, коли він далеко відійде або сховається за рогом.

Подальше переслідування чиниться без суєти і квапливості. Оптимальною позицією для спостереження за об'єктом при русі пішим порядком вважається розташування за спиною ОС, яка надає повну свободу дій. Безпосередньо за об'єктом рухається лише одна людина, решта членів бригади ЗС розміщуються ззаду у вигляді розтягнутого Ланцюжка, причому кожен з подальших орієнтується по попередньому.

В обов'язковому порядку при роботі у складі бригади ЗС один з детективів зобов'язаний рухатися по протилежній стороні вулиці паралельно об'єкту, контролюючи його можливі повороти на перехрестях і відхід в прохідні двори. Це дозволяє здійснювати якісніший контроль об'єкту, не даючи йому можливості сховатися на перехресті.

Відстань, з якої ведеться спостереження, залежить від багатьох причин. Воно може змінюватися від трьох—п'яти метрів на жвавих вулицях або руху в натовпі, до п'ятидесяти - ста метрів на малолюдних і пустинних вулицях, де достатньо бачити об'єкт здалеку.

Рух за об'єктом здійснюється як по тій же стороні вулиці, що і ОС, так і по протилежній. Темп руху спостерігача повинен відповідати швидкості руху об'єкту. При повороті ОС за ріг вулиці, швидкість руху прискорюється.

При роботі поодинці у разі, коли об'єкт ховається за рогом будівлі, не слід наздоганяти його бігом, треба перейти на протилежну сторону вулиці і прискорити крок. Якщо при виході із-за повороту ОС не вдається виявити, то необхідно ретельно проаналізувати, куди міг укритись об'єкт: номер будинку, якщо вдається, то і квартиру, за час, коли він знаходився поза зоною візуального контролю спостерігача. Найчастіше це бувають магазини, під'їзди, прохідні двори і т.п.

При втраті об'єкту найближчий район охоплюється кільцем, що поступово стискається, із членів бригади спостереження. Після виявлення ОС детективи поступово розтягуються в стандартний ланцюжок.

Якщо об'єкт пішов з-під спостереження, повинні бути узяті під контроль: місця можливої появи об'єкту (адреси мешкання родичів коханки, друзів, постійно відвідувані ресторани і кафе, місце роботи і таке інше).

Слідуючи за об'єктом, детектив повинен уміти засікати свій об'єкт в натовпі: вивчити його ходу, характерні рухи, переважні маршруту руху і т.д. Щоб ретельно розглянути особу спостережуваного, потрібно використовувати багатолюдні вулиці і перехрестя, оптові ринки, суспільний

транспорт і т.д., оскільки в цих місцях це можна виконати непомітно» для ОС.

Якщо зустріч з об'єктом неминуча, то необхідно ухилятися навіть від моментальних поглядів з об'єктом ока в око. Такі речі дуже легко запам'ятовуються. В процесі роботи спостерігач повинен зберігати незворушний вираз обличчя і показну байдужість.

При русі ОС пішим порядком бригада ЗС може рухатися, розтягнувшись в мережу, хтось попереду, інші паралельними вулицями і провулками, прохідними дворами, підтримуючи зв'язок з машиною і один з одним.

Якщо об'єкт починає нервувати і постійно озирається, необхідно ретельно проаналізувати, чому це відбувається: чи то у нього в даний момент призначена зустріч, і він вважає за краще підстрахуватися, чи то ОС виявив ЗС. У першому випадку рекомендується продовжувати спостереження, підсиливши заходи маскування, в другому — тимчасово зняти спостереження з об'єкту.

Довівши об'єкт до житлового будинку, необхідно обстежити його двір – чи не має він декількох виходів і якщо має – перекрити їх всі.

Ознаками повернення об'єкту додому можуть служити наступні спостереження : упевнене орієнтування на місцевості, знання цифр кодового замку на дверях під'їзду, винесення сміття, вихід за продуктами і т.п. Якщо подібних чинників не відмічено, то іноді можна під слушним приводом завести обережну розмову з пенсіонерами біля під'їзду (особливо в багатоквартирних будинках, де низька вірогідність розшифровки) з метою отримання додаткової інформації.

З'ясувавши місця відвідин ОС, необхідно твердо запам'ятати, а при першій слушній нагоді – записати: час перебування, приходу і відходу, вулицю, номер будинку, якщо вдасться, то і квартиру.

Супровід об'єкта спостереження при відвідинах ним місць масових зібрань

При відвідинах ОС організації або установи, детектив супроводжує його по будівлі тільки в тому разі якщо немає можливості візуального контакту через скло вікон і дверей.

Якщо ОС використовує ліфт, детективу не слід підніматися в одному ліфті з об'єктом, оскільки велика вірогідність запам'ятовування ОС зовнішності спостерігача. Визначивши по покажчику поверх підйому

ліфта, потрібно піднятися поверхом вище або нижче для пошуку ОС і його подальшого контролю.

В цілях виключення вірогідності відходу ОС з-під спостереження, члени бригади НН, що залишилися, здійснюють візуальний контроль всіх виходів з будівлі.

При відвідинах ОС ресторану або кафе, спостереження здійснюється одним співробітником ЗС або «сімейною» парою. Пройти в приміщення краще разом з іншими відвідувачами і під їх прикриттям зорієнтуватися, оцінити розташування приміщення, вибрати і зайняти зручну для спостереження позицію. Якщо ОС зайшов тільки з метою поїсти, то краще всього просто покинути приміщення, якщо об'єкт явно когось чекає, то, замовивши для обгрунтування свого знаходження декілька блюд, необхідно продовжувати спостереження за об'єктом і його співбесідником. Слід уникати розмов з відвідувачами, що випадково опинилися за одним столиком.

Рахунок краще сплатити заздалегідь, щоб не привертати увагу об'єкту і обслуговуючого персоналу своїм несподіваним відходом.

Відмітивши, що об'єкт збирається йти, потрібно спокійно закінчити прийом їжі. Спокійно встати і також спокійно вийти. Якщо ВІН все ще знаходиться в кафе або ресторані, то особливо важливо не зриватися різко услід за ним. При роботі в парі украй недопустимі відверті жести у бік об'єкту і слова типу «йде, пішли». Для психологічної підготовки вухо та підійде спокійно сказана фраза: «Чи не пора додому?» «Нас чекають удома» і т.д., щоб випадкові сусіди нічого не запідозрили.

Після виходу об'єкт найчастіше передається іншим членам бригади ЗС, а детективи, що «засвітилися», знімаються з подальшого спостереження в цілях виключення можливості розшифровки ЗС об'єктом.

При проведенні заходів щодо ЗС на залізничних, річкових і морських вокзалах і в аеропортах бригада ЗС повинна з'являтися на місці не пізніше, ніж за годину від відходу потягу, судна або відльоту літака і не пізніше, ніж за півгодини до їх прибуття.

Ведення ЗС в даному випадку здійснюється одним-двома детективами в максимальній близькості від об'єкту, решта членів бригади ЗС контролює наявні входи і виходи.

При несподіваному від'їзді ОС супроводжуючі його детективи повинні при першій же нагоді зв'язатися з керівництвом або замовником по

телефону або телеграфу. Використання в різних містах єдиних систем мобільного зв'язку дозволяє значно спростити цей процес.

Супровід об'єкту спостереження в міському транспорті

При використанні ОС міського транспорту (автобус, тролейбус або трамвай), спостереження ведеться одним детективом, який контролює дії об'єкту і по мобільному зв'язку інформує рухому на відстані автомашину з рештою бригади ЗС. Протягом поїздки треба визначити — чи не спостерігає об'єкт за тими, хто сідає і виходить з транспорту услід за ним. У випадку, якщо ОС обертає на це увагу, то з міркувань можливої розшифровки подальше переслідування чиниться в автомашині бригади ЗС або у таксі, уважно спостерігаючи за тих коли об'єкт сідає або покидає транспортний засіб.

У метро доцільніше використовувати двох чоловік, один з яких слідує в одному вагоні з об'єктом ЗС, інший — в сусідньому вагоні.

Супровід об'єкту спостереження, слідуючого залізничним або авіатранспортом

Для супроводу ОС, наступного залізничним або авіатранспортом, використовується не менше двох детективів, тільки в цьому випадку може бути забезпечений успіх заходів, що проводяться, і усунені небажані випадковості (втрата ОС, розшифровка детектива і т.д.).

Якщо ОС не показує зовнішнього неспокою, то детективам бажано помістится з ним в одному вагоні (у різних купе), зайняти зручну позицію і звідти вести спостереження. Встановлювати місце призначення поїздки об'єкта треба дуже обережно, а у разі неможливості отримання даної інформації, необхідна покупка квитка до кінцевої станції.

У літаку одному детективу слід зайняти позицію біля виходу, а іншому — в кінці салону.

В дорозі один детектив не спить, інший відпочиває. При наближенні до кожної станції або місця проміжної посадки необхідно дуже обережно перевірити — чи не збирається об'єкт покинути транспортний засіб.

Після прибуття ОС на місце, один з детективів зобов'язаний проінформувати керівництво або замовника про точку свого знаходження в зашифрованій формі по міжміському телефону або телеграфу.

При прибутті детективів в нове місто, необхідно в перший же вільний годинник зайнятися його вивченням, тобто придбати його карту, схеми руху суспільного транспорту, дізнатися вулиці, суспільні місця,

місце розташування залізничних, морських і автовокзалів, аеропортів, отримати графіки руху транспорту.

У зв'язку з навколишнім оточенням, що змінилося, необхідно змінити, відповідно ній, свій зовнішній вигляд. Якщо прихоплений в дорогу одяг сильно відрізняється від загальноприйнятого в даній місцевості, необхідно придбати нову одежу, бажано вже вживану, але і несильно заношену.

Людина, одягнена з голови до ніг в абсолютно новий одяг, завжди викликає підозру.

У разі втрати ОС один з детективів продовжує розшукувати його в місцях, які той часто відвідував до цього, а інший намагається виявити сліди від'їзду ОС з міста на вокзалах і аеропортах.

Супровід об'єкту спостереження при використанні ним автотранспорту

ЗС за об'єктом, що пересувається на автотранспорті, вимагає від детективів залишатися непомітними для нього (і бажано для всіх останніх), не порушуючи при цьому правил дорожнього руху. Це дуже складне завдання, особливо, коли об'єкт знайомий з методами виявлення ЗС і застосовує їх (порушення) для відриву від нього, для цього виду спостереження зазвичай використовується декілька автомашин.

Щоб не потрапити на очі ОС, можливі різні методи маскування то відставання машини ЗС, то рух по паралельних вулицях і провулках, використання прохідних дворів.

При русі по шосе застосовується наступна схема спостереження за об'єктом: одна з машин ЗС рухається попереду об'єкта, ще одна на деякому видаленні від нього (але на відстані візуального контролю) і ще одна авто машина ЗС замикає ланцюжок. При зупинці об'єкту, переслідуюча його машина ЗС проїжджає мимо і по радіозв'язку попереджає своїх колег про зупинку об'єкту і передаючи його їм під спостереження. Аналогічно відбувається при різкому збільшенні об'єктом спостереження швидкості. Функції спостерігача передаються попереду їдучій машині.

При переслідуванні об'єкту по шосе однією автомашиною по всьому маршруту рекомендується оснастити автомобіль об'єкту спостереження радіомаяком.

Автотранспортні засоби, використовуючи при веденні зовнішнього спостереження

Використовуючи при веденні ЗС автотранспортні засоби повинні сприяти виконанню поставленого завдання, не привертаючи до себе уваги з боку ОС. Тому в роботі по спостереженню переважно використовувати автомобілі вітчизняних марок, вони менш привертають до себе увагу, як об'єкту спостереження, так і вуличних роззяв і пенсіонерів у дворах будинків. Оптимальним вибором для роботи в міських умовах є ВАЗ-2106.

Автомашина повинна бути нейтральних тонів і не виділятися в транспортному потоці або на автостоянці. У міських умовах колір автотранспорту, що найбільш не запам'ятовується, — сірий або бежевий, до того ж в темний час доби автомашини подібного кольору дуже добре зливаються із загальним фоном. Влітку в районах з великою кількістю зелених насаджень доцільно використовувати автомобілі темно-зеленого і темно-блакитного кольорів. В крайньому випадку, допустиме використання автотранспорту спокійних тонів. Жодною мірою неприпустимо використовувати АТ засобу червоного, оранжевого, жовтого, білого і близьких до них тонів, а також тонів, що є особливо модними цього сезону.

Необхідно позбавитися від всіляких автомобільних прикрас (наклейок, емблем, іграшок і строкатих шторок на вікнах), від нестандартних елементів обробки автомобіля і великих, таких, що впадають в очі, антен.

Використовуваний засіб АТ повинен бути чистим і не мати вм'ятин, на корпусі не повинно бути подряпин або вищербин. Категорично виключається використання автотранспорту з шпаклювальними плямами.

Технічний стан автомашини — предмет окремої розмови. Перед виходом на завдання АТ засіб повинен бути ретельно оглянутий, перевірені гальма, акумулятор, наявність запасного колеса і необхідного набору інструментів. Важливим і невід'ємним атрибутом є автомобільна аптечка.

Перш ніж використовувати автомашину в заході щодо ведення ЗС, необхідно з'ясувати її граничну швидкість, гальмівний шлях, мінімальний радіус розвороту, витрату палива і т.д. Перед кожним виїздом на операцію необхідна ретельна перевірка технічного стану автомобіля.

Технічні засоби ведення зовнішнього спостереження

При веденні ЗС використовуються різні технічні засоби. До них відносяться:

- бінокли, оптичні приціли, стереотруби і інші системи візуального спостереження, що дозволяють контролювати ОС при звичайному освітленні в межах певної видимості;
- відеосистеми спостереження;
- інфрачервоні системи і прилади нічного бачення, використовуючи в умовах обмеженої видимості або в темний час доби.

Подібні технічні засоби використовуються як в побутового виконання (використання техніки, яка продається в звичайних магазинах, менше привертає увагу тих, що оточують), так і в спеціального (що камуфлює) виконання (бінокли з вбудованим фотоапаратом, приховані телекамери і ін.).

Для ведення ЗС за рухомими засобами, наприклад, за маршрутом руху автомобілів, в них можливий прихований монтаж радіомаяків, що дозволяють бригаді ЗС визначати відстань до спостережуваного транспортного засобу або за допомогою пеленгаторних пристроїв визначати місцезнаходження з певним ступенем точності.

Аналітична обробка результатів зовнішнього спостереження

Дані, отримані в результаті ведення ЗС, повинні фіксуватися в журналі спостережень при стаціонарному спостереженні і в звітах про виконану роботу при спостереженні рухомого об'єкту. Отримана інформація повинна відповідним чином сортуватися, систематизуватися і аналізуватися. Основне призначення всіх аналітичних методів - обробка зібраної інформації, встановлення взаємозв'язків і виявлення причинно-наслідкових зв'язків зібраних фактів і явищ для остаточного звіту про виконану роботу.

До вже зібраного інформаційного масиву результатів спостережень доцільно прикласти фотографії, матеріали відеозйомки, діаграми зв'язку, матриці контактів ОС, тимчасові графіки і графіки аналізу візуальних спостережень і оцінки результатів.

Для прискорення процедури аналітичної обробки інформації доцільне застосування комп'ютерної техніки і зведення результатів спостережень в електронні бази даних.

За відсутності техніки можливий "ручний" аналіз.

У асоціативних графіках застосовуються цифри, таблиці і геометричні фігури для демонстрації зв'язків між об'єктом спостереження і його потенційно можливими і дійсними контактерами. За допомогою

асоціативних діаграм виявляються області ділових і особистих інтересів ОС - хобі, спорт, культурні інтереси, оточення, місця мешкання і відвідин з одними і тими ж особами (автотранспортними засобами) в різних точках маршруту руху.

Виявлення зовнішнього спостереження (ЗС)

Виявлення ЗС здійснюється шляхом ретельного вивчення навколишнього оточення, з акцентуванням уваги на неодноразові зустрічі з одними і тими ж особами (автотранспортними засобами) в різних точках маршруту руху.

Ви повинні прагнути до того, щоб ваше сприйняття навколишнього оточення поступово ставало машинальним, таким, що автоматично фіксує будь-який підозрілий факт: незнайома автомашина в звичному провулку, людина, яка начебто читає газету, але що зовсім не обертає на неї уваги, жінка в будці телефону-автомата, що розмовляє з кимось не набираючи номера і що одночасно уважно спостерігає за під'їздом навпроти.

Дуже часто ЗС ведеться не тільки за дверима вашого під'їзду або входу до установи, де ви працюєте, але і за вашими вікнами, тобто ви ще тільки починаєте надягати пальто, а бригада ЗС вже чекає, коли ви покажетеся з під'їзду.

Виявлення ЗС може бути "грубим" і "м'яким". Для "грубого" стилю виявлення ЗС характерне регулярне "зав'язування" шнурків, періодичний огляд що відбувається за спиною шляхом постійного огляду, а також раптові контакти з особами, ведучими спостереження.

Осіб, ведучих ЗС, особливо якщо це не професіонали, характеризує скутість рухів, хвилювання, прагнення не зустрічатися поглядом з об'єктом спостереження, використання засобів оперативного зв'язку (радіостанцій, мобільних телефонів), неприродні пересування і спроби сховатися за укриття або людей.

При веденні ЗС зміна нижньої частини одягу (у чоловіків - шкарпеток, черевик, брюк, у жінок - колготок, туфель, спідниць) значно утруднена, що також дає можливість для розшифровки можливого ЗС.

Невиправдане тривале знаходження людей без видимих причин в автотранспорті і порушення ними правил дорожнього руху також може свідчити про спостереження, що ведеться за вами.

Проте перш ніж, ви прийдете до твердого переконання, що за вами стежать, вам необхідно виконати два простих правила.

По-перше, необхідно реально оцінити таку річ, як ступінь вірогідності спостереження за вами і спробувати проаналізувати мету його проведення і вірогідних замовників.

По-друге, вам потрібно буде перевірити ще раз вашу гіпотезу про спостереження, що ведеться за вами. Тільки після зіставлення гіпотези з передбачуваними і виявленими додатковими спостереженнями, фактами і фактами ви зможете з деякою надійністю стверджувати, що за вами дійсно стежать. Виявлення ЗС в процесі руху пішим порядком, як і все пов'язане із забезпеченням вашої безпеки, припускає творчий підхід.

"М'яке" виявлення зовнішнього спостереження

Виявлення ЗС в процесі руху пішим порядком, як і все пов'язане із забезпеченням вашої безпеки, припускає творчий підхід. Перш за все необхідно ретельно розробити перевірочний маршрут і "легенду", підтверджуючу його виправданість, тобто кожна точка вашого маршруту повинна бути якось прив'язана до ваших службових обов'язків і ділових інтересів, особистих потреб і потреб. Будь-які нелогічні відхилення від вашого постійного графіка (якщо ви його дотримуєтеся) можуть викликати у ваших переслідувачів певні підозри і примусити їх діяти тонше і обережно, що значно ускладнює завдання по виявленню ЗС. Щоб це не відбувалося, прагніть уникати стереотипів в своїй поведінці, варіюйте час виходу з будинку, не використовуйте щодня одну і ту ж дорогу при русі на роботу і з роботи.

Для того, щоб якісно перевірятися і заразом утруднити ведення ЗС, необхідно розробити декілька маршрутів руху. Виявлення ЗС на короткому маршруті і за невеликий проміжок часу досить скрутно. Оптимальний час якісної перевірки варіюється в межах від години до півтора. Рух по вибраному маршруту пішим порядком повинно поєднуватися з посадками в суспільний транспорт. Останнє служить двом цілям: по-перше, ви примушуєте ваші переслідувачі понервувати із-за боязні вас втратити в товкучці і, по-друге, розробляючи маршрут, вибираючи вулиці з жвавим рухом, ви утруднюєте координацію їх дій.

У великих містах, де є метрополітен, дуже ефективно використовувати його в цілях відходу від ЗС. Як правило, бригада спостереження ділиться на дві частини одна - дві людини супроводжує об'єкт ЗС пішки, інші знаходяться в автотранспорті і слідують на нім за об'єктом. Члени бригади НН, що знаходяться в автомашині, координує, свої дії з колегами

по радіозв'язку, прагнучи прибути у вказану крапку з випередженням. Тому маршрут руху на метро потрібно вибирати у такий спосіб, щоб використовувати ті лінії, які проходять під водою, вулицями і проспектами з інтенсивним рухом і частими автомобільними пробками. При правильному виборі маршруту автомобіль бригади ЗС програє потягам метро в оперативності. Бригада ЗС виявляється роз'єднаною і розкиданою по місту. У цей момент і можна скористатися заздалегідь приготованим "сюрпризом" для відходу з-під спостереження.

Відсікання автомашини бригади ЗС можливо і при використанні такого тактичного прийому, як рух пішки по вулиці з одностороннім стрічним рухом. Поки автомобіль з бригадою ЗС шукатиме об'їзд ви залишаєтеся із спостерігачем один на один, що значно полегшує як виявлення ЗС, так і відхід з-під нього.

Дуже ефективний прийом - перехід на протилежну сторону вулиці. Особливо високі результати цей прийом показує в місцях з невеликою кількістю перехожих.

Методика перевірки достатньо проста. Рухаючись по заздалегідь певному маршруту, ви підходите до кромки тротуару, дотичному з проїжджою частиною, і обертаєтеся у бік транспорту, що наближається, з цілком зрозумілою метою огляду проїжджої частини з тим, щоб переконатися в безпеці переходу через вулицю. Протягом трьох-п'яти секунд ви спокійно можете розглядати вулицю, а також людей тих, що потрапили в полі вашого зору. Всіх їх рекомендується запам'ятати, щоб при подальшому попаданні їх вам на очі по частоті повторюваності можна було б судити про їх дійсний інтерес до вас.

Для виявлення ЗС широко застосовується прийом з використанням телефону-автомата. Рухаючись по вулиці, ви заходите в телефонну будку і, набираючи номер, як би ненавмисно обкидаєте поглядом пройдений шлях, запам'ятовуючи там все саме значуще. Найбільш ефективне використання телефонів-автоматів, розташованих відразу ж за рогом будівлі або усередині його арки.

Продумавши, перевірочний маршрут руху, виберіть декілька відрізків шляху, де б ви проходили мимо вітрин магазинів і кіосків так, щоб в них дзеркально відбивався напрям вашого руху. В даному випадку ви, не викликаючи підозр, можете роздивлятися вміст прилавків і попутно спостерігати за діями наступних за вами людей.

Нерідко магазини бувають розташовані на деякому піднесенні і для того, щоб туди потрапити, доводиться підніматися по сходинках, направлених убік, зворотну вашому первинному руху. Тут також надається маса можливостей по перевірці наявності "хвоста".

Самі магазини також є прекрасною можливістю для виявлення спостереження. Пересуваючись з відділу у відділ, від прилавка до прилавка, пробиваючи чек в касі, є маса можливостей змінити напрям руху і візуально оцінити людей, що йдуть назустріч.

З великим ефектом можна використовувати входи в магазини, що знаходяться в підворіттях або кутах будівель. ваше раптове зникнення там примушує переслідувачі понервувати, і як наслідок цього, розкрити себе, наприклад, прискоренням кроку, безпричинним метанням по вулиці, безцеремонним розгляданням перехожих.

Ви ж, знаходячись в укритті, через вікна або скляні двері маєте можливість вірно ідентифікувати спостереження, що ведеться за вами.

Виявлення зовнішнього спостереження (ЗС) в міському транспорті

Входити в суспільний транспорт (трамвай, автобус, тролейбус) рекомендується із заднього майданчика, там же краще і знаходитися під час всієї подальшої поїздки, щоб не тільки візуально контролювати ваш салон транспортного засобу, але і мати можливість контролю транспорту рухомого паралельно вашому маршруту.

Звичайно особа, що веде спостереження, також заходить із заднього майданчика і прагне зайняти позицію за вашою спиною, щоб виключити можливість втратити вас із виду, особливо при зупинках.

Знаходячись в міському транспорті, не привертаючи до себе уваги, уважно оцініть обстановку. Пам'ятаєте, при забезпеченні власної безпеки дрібниць не буває, адже як говорив старина Мюллер "маленька брехня, народжує великі підозри".

Особи, ведучі спостереження, через професійну специфіку уникають не тільки прямих поглядів, але і будь-яких візуальних контактів з об'єктом спостереження. Якщо хтось принципово не хоче зустрічатися з вами поглядом і ховає очі при будь-якому повороті в його сторону, візьміть собі це на замітку і, перевіривши ще раз отриману інформацію, дійте згідно обстановці, що складається.

Виявлення можливого зовнішнього спостереження при проведенні заходів щодо контрспостереження

Контрспостереження є найефективнішим прийомом виявлення "чужого" зовнішнього спостереження. Сенс контрспостереження полягає в розстановці в певних контрольних точках маршруту руху об'єкту контрспостереження (ОКС) постів КВС (контролю візуального спостереження). Пост КВС повинен бути відповідним чином укритий із надійною легендою... Оптимальним укриттям для нього є під'їзди довколишніх будинків, магазини, кафе, автомобілі. Спостерігачі повинні зайняти свої позиції за 30-40 хвилин до проходження об'єктом контрспостереження позначеної контрольної точки маршруту і покинути їх через 30-40 хвилин після її проходження. В процесі контрспостереження повинні фіксуватися всі невідповідності в зовнішності і поведінці тих, що знаходяться в зоні візуального контролю поста людей, транспортних засобів, ознаки спостереження, що ведеться, з довколишніх будівель і будов, транспортні засоби з одним або декількома пасажирами, що покидають зону візуального контролю відразу після проходження ОКС.

При проведенні заходів щодо контрспостереження, наприклад, в цілях контролю можливого ЗС з боку кримінальних структур за керівництвом фірми, рекомендується звертати увагу на наявність в припаркованому автотранспорті великої кількості головних уборів, "зайвого" верхнього одягу, термосів і судин з широким горлом. Також необхідно уважно спостерігати за зашторених вікнами довколишніх будівель з метою виявлення чи не ведеться з них ЗС, фото- і відеозйомки.

"Відхід на дно". Бувають випадки, коли в цілях особистої безпеки необхідно відірватися від жорсткого контролю з боку кримінальних угрупувань. "Відхід на дно" має на увазі під собою повне недопущення отримання кримінальним угрупуванням будь-якої інформації про об'єкт переслідування.

На попередньому етапі необхідно ретельно проаналізувати: хто, як, і з якою активністю вас шукатиме і, грунтуючись на цих даних, виробити спосіб відходу з-під спостереження і схему поведінки надалі.

У простому випадку це просте перебазування в інше місце проживання, ніяк не пов'язане з минулими контактами і біографією. Характеризується різким перериванням всіх підтримуваних донині особистих і ділових контактів, обов'язковою зміною зовнішнього вигляду (зачіска, окуляри, відпускання або гоління вусів і бороди, усунення старих і придбання нових звичок і пристрастей).

Психологічні моменти по нейтралізації можливого зовнішнього спостереження

Більшість людей, потрапляючи в незнайому обстановку, випробовують душевний дискомфорт, який намагаються зняти спілкуванням з випадковим попутником або сусідом по готельному номеру. Відверті бесіди з незнайомими людьми чреваті найнесподіванішими наслідками, адже попутники і сусіди можуть виявитися зовсім не тими, за кого себе видають. Дуже часто "випадкові" знайомства бувають достатньо чітко сплановані і організовані. Рада тут може бути тільки один - обережність, обережність і ще раз обережність.

Наступним психологічним моментом, що полегшує ведення ЗС, є формування у людей стійких звичок і стереотипів. У багатьох випадках по знайомій нам місцевості ми рухаємося, як би на "автопілоті", дуже часто не помічаючи те, що відбувається навколо нас. Час і маршрути руху повинні регулярно мінятися. Розпорядок робочого дня повинен ретельно легендуватися. І взагалі, чим більше в поведінці людини незвичних і непередбачуваних дій, тим сильніше ускладнюються завдання зовнішнього спостереження.

Для отримання попередньої інформації можуть використовуватися телефонні дзвінки від імені знайомих додому, за місцем роботи, колегам і друзям, інформованим про ваш розпорядок дня. Зовнішнє спостереження – це один із методів роботи служби безпеки, тому ми цьому розділу приділимо більше уваги на семінарських заняттях.

Розділ 6.

Несумлінна конкуренція і взаємовідносини між суб'єктами

Програмна анотація

6.1. Менеджмент діяльності по захисту від несумлінної конкуренції

– методи і засоби несумлінної конкуренції.

6.2. Примусове злиття підприємства

– як відстояти свою незалежність ?

6.3. Зовнішні джерела погроз організаційній діяльності

– відомості, що складають комерційну таємницю,

– конфлікт інтересів сторін,

– інформаційні взаємовідносини між суб'єктами,

– висновок і пропозиції.

6.1. Менеджмент діяльності по захисту від несумлінної конкуренції

Під терміном «несумлінна конкуренція» розуміють порушення загальновизнаних правил і норм ведення конкурентної боротьби: використання конфіденційної інформації; розповсюдження недостовірної інформації; приховування важливої для споживача інформації, демпінг (тобто продаж на зовнішньому ринку товару за ціною, нижчою від існуючої на внутрішньому ринку країни-експортера) тощо.

Центральним поняттям, що виражає сутність ринкових відносин є поняття конкуренції (competition). Конкуренція - це найважливіша ланка всієї системи ринкового господарства. Стимулом, що спонукає людину до конкурентної боротьби, є прагнення перевершити інших. Предметом конкурентного суперництва на ринках є частки ринку, контрольовані тими чи іншими товаровиробниками. Конкурентна боротьба - це динамічний процес. Він сприяє ліпшому забезпеченню ринку товарами.

В якості засобів в конкурентній боротьбі для поліпшення своїх позицій на ринку компанії використовують, зокрема, якість виробів, ціну, сервісне обслуговування, асортимент, умови поставок і платежів, рекламу.

Створення конкурентного середовища й подолання монополізму є одним з найважливіших напрямів економічної реформи в Україні. Ще в Законі про економічну самостійність України (серпень 1990 р.) та в постанові Верховної Ради "Про проекти концепції та програми переходу Української РСР до ринкової економіки" (листопад 1990 р.) "передбачалося провести роздержавлення і приватизацію, створивши справжнє підприємницьке середовище і ринкову конкуренцію". Проте здійснена в Україні приватизація ще не призвела до створення сприятливого для економічного зростання конкурентного середовища.

Схоже на те, що "обмеження діяльності підприємств-монополістів для цього недостатньо, поза як в наш час більше половини великих підприємств є монополістами у своїх галузях, і тому тільки приватизація, розкрупнення там, де це можливо, й зацікавленість у розвитку альтернативних недержавних виробництв може забезпечити нормальну конкуренцію на українському ринку».

Сумлінна та несумлінна конкуренція, методи ведення промислового шпигунства

Сумлінна конкуренція

З огляду на засоби, які застосовують суперники в конкурентній боротьбі конкуренцію можна умовно поділити на сумлінну й несумлінну.

Основними методами сумлінної конкуренції є:

- зниження цін (“війна цін”);
- підвищення якості продукції;
- розвиток до й після продажного обслуговування;
- створення нових товарів і послуг з використанням досягнень НТР тощо.

Несумлінна конкуренція.

Поряд з методами сумлінної конкуренції існують і інші, менш законні, методи ведення конкурентної боротьби – несумлінна конкуренція:

Основними методами несумлінної конкуренції є:

- економічне (промислове) шпигунство;
- підробка продукції конкурентів;
- підкуп і шантаж;
- обдурювання споживачів;
- махінації з діловою звітністю;
- валютні махінації;
- приховування дефектів тощо.

До цього можна також додати й **науково-технічне шпигунство**, оскільки будь-яка науково-технічна розробка тільки тоді є джерелом прибутку, коли вона знаходить застосування в практиці, тобто коли науково-технічні ідеї втілюються на виробництві в вигляді конкретних товарів або нових технологій.

Саме промислове шпигунство, так би мовити, "створило" патент на винахід. Так як зберегти секрети виробництва не вдавалось, винахідник, витративши роки праці, міг і не одержати жодної винагороди за свій винахід, адже з результату винаходу часто користалися цілковито сторонні люди, що не мали жодного відношення до винаходу.

Запобігти такій несправедливості мав патент, що посвідчує винахід і закріпляє за власником патенту виключне право на користування результатами свого винаходу. Якщо патент використовується без дозволу власника, власник може за допомогою суду відшкодувати збитки або припинити незаконне користування його винаходом. Крім того, він може видати ліцензію іншим особам на використання запатентованого винаходу.

Але патент, теоретично спрямований проти промислового шпигунства, практично став свого роду стимулом цього явища. Один з перших законів про патенти на винахід було видано у Франції наприкінці XVIII століття, в ньому передбачалося, що за всяким, хто першим привезе у Францію якийсь іноземний винахід, визнаються такі самі пільги, якими б користувався його винахідник.

Таким чином, за промисловим шпигуном визнаються права, рівні правам винахідника.

Часто терміни "промислове шпигунство" та "економічне шпигунство" застосовують як синоніми. Але між ними існує певна відмінність, адже промислове шпигунство, зрештою, є частиною економічного.

Економічне шпигунство, крім промислового, охоплює й такі сфери, як показники валового національного продукту, тобто сума доходів підприємств, організацій і населення в матеріальному й нематеріальному виробництві й амортизаційних відрахувань), його розподіл по галузях економіки, процентні ставки, запаси природних ресурсів, можливі зміни в технічній політиці, проекти створення великих державних об`єктів - заводів, полігонів, магістралей тощо.

Відповідь на питання, чому в центрі уваги економічного шпигунства виявляються вище перелічені показники держави, полягає в тому, що

багато країн дають узагальнені дані, з яких важко встановити формування доходів і видатків тої чи іншої галузі або всієї держави. Особливо це відноситься до таких сфер, як фінансування різного роду науково-дослідницьких робіт в області ядерної фізики й електроніки, космічної промисловості і т.і.

Основними об'єктами уваги промислових шпигунів є патенти, креслення, секрети виробництва, технології, структура витрат; економічне шпигунство крім промислових секретів охоплює й макроекономічні показники і вбирає в себе розвідку природних ресурсів, виявлення промислових запасів; у зв'язку з розвитком маркетингу великої цінності набуває збирання інформації про смаки й доходи різних соціальних груп.

З розвитком промислового шпигунства монополістичні фірми ретельно охороняють зміст патентів, результати науково-технічних досліджень, проекти і ескізи будь-якої своєї продукції. В організаційну структуру транснаціональних корпорацій (ТНК) входять так звані технічні центри, основним завданням яких є розробка нових товарів, підвищення якості вже існуючої продукції, розробка нових технологій тощо.

З метою підвищення прибутку ТНК прагнуть до встановлення істинної цінності власної продукції. Для цього здійснюється детальний аналіз продукції конкурентів для встановлення порівняльної якості своєї продукції.

Всі промислові монополії мають засекречені лабораторії, де по всіх параметрах порівнюють рівні технічних рішень, якість, продуктивність і надійність своєї продукції з аналогічною продукцією конкурентів. В цих лабораторіях розбирають кожен вузол і агрегат власних машин і аналогічної продукції конкурентів, щоби об'єктивно порівняти їх і виявити дійсну цінність тої чи іншої продукції. Враховуються всі недоліки та переваги своїх і чужих товарів. Все ліпше в конкурентів переймають і пристосовують для своїх машин, механізмів і конструкцій, якщо при цьому можна обминути патентне законодавство або якщо це вигідно фірмі.

Недоліки своєї продукції ретельно вивчаються. Потім шукаються шляхи їх усунення, якщо це виявляється вигідно. Але ніколи інформація про слабкі сторони своєї продукції не виходить за межі таких лабораторій і, звичайно, ніколи не доходить до звичайних споживачів. Саме існування таких лабораторій також не афішується.

Існують різні способи здобуття конфіденційної інформації про діяльність конкурентів, як законних, так і незаконних. Законними засобами вважаються збирання й аналіз інформації з офіційно-опублікованих джерел, доповідей, звітів, вивчення продукції конкурентів тощо.

Основними законними шляхами збирання інформації про конкурентів є: публікації конкурентів і звіти про діяльність фірм; відомості, що дали публічно колишні службовці конкурентів; щорічні фінансові звіти; огляди ринків і доповіді інженерів-консультантів; видання, що їх видають конкуренти; аналіз виробів конкурентів; звіти зарубіжних філій тощо.

Так як кожна ТНК знає про можливі дії проти неї конкурентів, дослідження, здійснювані ними, то в офіційних публікаціях і звітах кожна ТНК намагається дати мінімальну інформацію про свою діяльність і фінансове становище, про науково-дослідницькі роботи. Здебільшого будь-яка велика компанія складає декілька варіантів звіту.

Звіт, що відбиває справжній стан справ, в лічених примірниках подається вищим керівникам ТНК, які визначають політику і стратегію корпорації.

Інший варіант звіту, з якого вилучена найбільш важлива інформація, структура виробничих витрат, подається керівникам корпорації середнього рівня, деяким управляючим зарубіжними філіями, деяким особам з середовища основних акціонерів.

Можливий і третій - популярний варіант звіту, в якому відсутній конкретний зміст, але присутні відмінні ілюстрації, звіт прекрасно видано тощо; такий звіт призначений для акціонерів і широкої громадськості.

Засоби несумлінної конкуренції

Але конкурентні фірми, знаючи про можливі способи приховування інформації, збирають конфіденціальну інформацію наступними шляхами:

- різноманітні питання, що ставляться спеціалістам конкурента;
- запрошення на роботу спеціалістів конкурента;
- удавані пропозиції роботи спеціалістам із фірм-конкурентів без наміру брати їх на роботу.

Також можуть бути реалізовані наступні засоби:

- таємне спостереження за спеціалістом, відділом, лабораторією конкурента;
- використання професіональних шпигунів для отримання інформації;

- підкуп співробітників з основних відділів фірми-конкурента;
- впровадження "потрібних" осіб в структуру фірми-конкурента;
- підслуховування розмов тощо;
- викрадення креслень, зразків, документів;
- шантаж та інші способи тиску;
- здобуття інформації від джерел у державних структурах;
- збирання інформації від зарубіжних філій і від спільних постачальників.

Ще одним ефективним способом економічного шпигунства є впровадження "своєї людини" в державні органи, покликані регулювати діяльність промислових монополій, що дозволяє одержувати необхідну інформацію про конкурентів, контролювати дії, пов'язані з антимонопольною політикою тощо.

Іншим засобом несумлінної конкуренції є **фальсифікація фірмової продукції**.

Ці дії також тісно пов'язані з патентуванням. З економічної точки зору патентування рівнозначно монополізації вигод, пов'язаних з використанням патенту.

Найчастіше патент надає реальні вигоди впродовж семи років, що дозволяє за цей час одержувати чималий прибуток його власникові. Але з іншого боку, поява патенту, що забороняє використовувати якийсь запатентований винахід безпосередньо конкурентами, спонукає їх до форсованої розробки якихось нових технічних прийомів, технологій.

Крім того, багато важливих винаходів часто не патентуються, щоби не привертати до них увагу конкурентів. Це здебільшого стосується технологій, технічних процесів, які тяжко скопіювати, на відміну від створення нових товарів

Шлях від винайдення до комерційного застосування вимагає великих фінансових, трудових і матеріальних витрат. Тому, якщо нема небезпеки, що конкурент не запровадить винахід швидше, ніж сама корпорація, то винахід не патентується, якщо ж існує ризик, що винахід буде використано конкурентом, то його відразу ж патентують і конкурент змушений 15-20 років очікувати, доки мине строк монопольного права. Секрети виробництва тих чи інших товарів не патентуються для того, щоби по закінченні певного строку не обнародувати технологію їх виготовлення. Наявність патенту служить потужним засобом для контролю над ринком,

поза як його порушення карається конфіскацією незаконно виробленої продукції, відшкодуванням збитків і сплатою порушником великих штрафів, що досягають 10 млн. доларів. Патенти застосовуються передовсім для охорони продукції фірми від підробок чи імітації якісних товарів.

Для фірм, чию продукцію копіюють, підробки мають катастрофічні наслідки: різко звужується ринок збуту, прибуток різко знижується, уходячи до виробників підробок, підробки підривають авторитет фірми, бо вони крім своєї дешевизни мають ще й низьку якість, тому підробки швидко виходять з ладу, погіршуючи в такий спосіб довіру споживачів до фірми, чия марка була підроблена.

Такий метод несумлінної конкуренції як сучасне промислове шпигунство користується новітніми досягненнями науки й техніки. Часто стали застосовуватися різні мікроскопічні прилади на основі електронних схем.

Розвиток комп'ютерного піратства й злодійства змусив уряди багатьох країн застосовувати різні заходи; наприклад, в США організована спеціальна група, що відповідає за безпеку й недоторканість комп'ютерних мереж і комп'ютерних баз даних, поза як будь-яка людина, що має комп'ютер, доступ у мережу та певні навички роботи з комп'ютером може здобути доступ у такі комп'ютерні банки даних, що містять конфіденційну й секретну інформацію, яка не призначена для рядового користувача. В якості прикладу можна навести випадок, що відбувся в США, коли один користувач зміг підключитися до мережі комп'ютерів міністерства оборони США, в результаті його злого наміру була повністю знищена важлива інформація одного з пентагонівських комп'ютерів.

6.2. Примусове злиття підприємства

Не одна компанія, або підприємство не застраховане від не дружелюбного поглинання – іншою.

Ми наголошуємо, що універсального захисту від навмисного злиття одного підприємства – іншим, не існує. Ми з вами знаємо, що на сьогоднішній день в

Україні залишилися без приватизації, тільки декілька великих підприємств, значить, кількість не дружелюбного поглинання один-одного, (несумлінних методів боротьби, конкуренції та інше) різко поповзе вгору.

Діло в тім, що існуюче Українське законодавство надає масу можливостей для таких поглинань, у той же час значно обмежуючи можливості захисту.

Захоплення підприємства

Спроба захоплення підприємства може мати кілька мотивів. Як правило, ці дії порозуміваються прагненням одержати доступ до ліквідних активів жертви (від устаткування до пізнаваної торговельної марки), її переважними правами (наприклад, право оренди). Ще одним мотивом недружнього поглинання може стати бажання вивести із гри конкурента. Коли невелика компанія здатна робити погоду на ринку, великим гравцям буває вигідніше неї поглинути, чим брати участь у конкурентній боротьбі. Існує ще трохи законних методів поглинання.

Перший етап.

1.) Скупка акцій. Найбільш уразливі в цьому змісті підприємства - відкриті акціонерні товариства. Один з розповсюджених способів їхнього захоплення - скупка акцій у акціонерів і власників невеликих пакетів. Спочатку поглиначі здобувають невелика кількість акцій, які дають власникові можливість брати участь у зборах акціонерів, звертатися до керівництва компанії з вимогою надати фінансову документацію, певним чином впливати на думки інших власників акцій.

2.) Ціль цього етапу - підготувати плацдарм для майбутнього поглинання й прощупати позиції нинішніх власників компанії.

На другому етапі поглинання акціонерного товариства, компанія-поглинач одержує контроль над все більшими пакетами акцій: спочатку блокують (більше 25%), потім контрольним (більше 50%+1 акція). Одержання контролю може йти по декількох сценаріях: шляхом як скупки акцій, так й одержання доручення на голосування від імені інших власників.

В ідеалі поглинач одержує в керування пакет акцій, що дозволяє одноосібно або за допомогою афілійованих осіб забезпечити на зборах акціонерів кворум (більше 60% акцій) і приймати будь-які рішення, у тому числі про збільшення статутного капіталу й відчуженні активів (для вне-

сення змін в устав або ухвалення рішення про ліквідацію підприємства необхідно більше 75% акцій).

Поглинання через процедуру

Ініціатором процедури банкрутства з потенційний поглинач. Основне завдання компанії-набувача це контролювати арбітражного керуючого, що може ввести мораторій на погашення боргів, арешт рахунків й активів.

Тоді процес може піти по сценарію поглинача. Навіть якщо підприємство починає виплачувати борги, це не означає миттєве припинення процедури банкрутства. Крім того, на прохання кредитора погашення боргів може здійснюватися тільки по згоді арбітражного керуючого, що, діючи в інтересах поглинача, своєї згоди не дасть.

Жах такого положення поглинає компанію, у тім, за визначенням суду арбітражному керуючому надаються досить широкі повноваження, при цьому відповідно зменшуються можливості дирекції. Якщо мова йде про поглинання заводу, звичайно його робота припиняється, триває лише відвантаження продукції, на яку вже були укладені контракти. Таким чином, гроші на рахунках лише накопичуються, але не витрачаються".

Звичайне підприємство не здатне оплатити всі борги, і в такому випадку можливі два варіанти.

1.) Коли арбітражний керуючий - це людина поглинача, а комітет кредиторів представляє інтереси ворожої сторони, підприємство може продовжувати роботу, але вже без участі колишніх власників.

2.) Далі треба включити процедуру санації, коли представники набувача повідомляють про готовність погасити борги, одержавши замість активи підприємства.

Штучні борги

Досвід показує, що навіть якщо підприємство цілком рентабельно, найчастіше можна знайти якийсь неоплачений, прострочений борг. Якщо такого не має, його створюють штучно або навіть фальсифікують.

Легше всього створити заборгованість, якщо є домовленість із менеджером компанії, яку поглинають, у цьому випадку керівник може, приміром , украсти який-небудь фіктивний договір і відстрочити його оплату, що дає підстави для судової суперечки. Причому позивач робить все можливе, щоб прийняте на його користь рішення не було виконано.

Адже якщо гроші вчасно не надійдуть іншій стороні, що виграла судовий процес з цього приводу, це може стати основою для подачі заяви

про банкрутство. Залишається домогтися винесення відповідного визначення суду, яким призначається арбітражний керуючий, а дирекція підприємства, що поглинає, відстороняється від ведення справ.

Далі ситуація розвивається як при звичайному банкрутстві: накладає мораторій на задоволення вимог кредиторів, сума боргів росте, і процедура банкрутства підприємства триває... Цей шлях займає рік-півтора, а контроль над підприємством можна встановити протягом декількох місяців.

Розбіжність в адресі підприємства

Якщо підприємство зареєстроване не по тій адресі, де воно фактично перебуває, загарбник може направити в суд позов з вимогою виплати якоїсь заборгованості або відшкодування збитку, або підрив ділової репутації. Неважливо, який саме позов і чим обґрунтовані вимоги, головне, щоб у ньому була зазначена не той адрес відповідача, де він фактично перебуває, а той, по якому він зареєстрований. В надії, що відповідач не з'явиться до суду.

У результаті, на засідання суду представники відповідача не з'являються, оскільки нічого не знають про процес, що почався. Рішення виноситься без їхньої участі. Через три місяці, якщо вимоги позивача не виконані, вони ініціюють процедуру банкрутства. Для поглинача головне, щоб відповідач нічого не знав про процес, що почався. А після початку процедури банкрутства оскаржити що-небудь уже пізно. Суд виніс рішення і змінити його – потрібно багато часу.

Свідомі акціонери

При поглинанні акціонерних товариств, найчастіше використають права самих акціонерів. Адже вони мають право звертатися в суд за захистом своїх прав, наприклад, з позовом про визнання незаконними рішень про збори акціонерів, призначенні директора, висновку договорів і т.п.. У будь-який момент такий акціонер може звернутися в суд з позовом про визнання якихось дій керівництва компанії незаконними.

Таким чином, можуть бути визнані недійсними результати тендера або договору про покупку якогось устаткування, якщо акціонер доведе, що в результаті цієї угоди защемлені його права. У цьому випадку активні акціонери можуть бути інструментом корпоративних війн.

При правильному використанні прав дрібних акціонерів можна істотно загальмувати й ускладнити роботу компанії. Теоретично ніхто не забороняє будь-якому громадянинові купити одну акцію будь-якого

акціонерного товариства й шляхом незліченних позовів перешкоджати його нормальній роботі. З іншого боку, керівництво компанії може використати свого ж акціонера як інструмент легалізації сумнівних угод. Наприклад, грамотний акціонер звертається в суд для визнання такої угоди незаконної, а суд, розглянувши справу, не знаходить ознак порушення закону.

Після того як рішення набутило чинності , і пройшов строк його оскарження, воно діє як охоронна грамота - цю угоду вже не можна визнати нелегітимної. Застосувавши цей прийом, підкуплений менеджер підприємства, що поглинає, здатний продати активи компанії-поглиначу. Свідомий «акціонер» подає позов у суд із заявою про порушення своїх прав, але суд підтверджує законність цієї угоди. Це також використовують в своїх інтересах.

Кадри - слабка ланка

У пострадянських країнах працює метод поглинання, суть якого у свій час озвучив Борис Березовський: "Нам немає потреби купувати «Логоваз», якщо ми можемо купити менеджмент Логоваза". Зацікавлена в поглинанні компанія зманює на своє підприємство фахівців і менеджерів, без яких робота підприємства, що поглинає, стає практично неможливою, потім використовують цих менеджерів. Переконавшись у цьому, власники компанії можуть стати поступливі і добровільно продати фірму.

Як відстояти незалежність

Раптове банкрутство. Захищатися від поглинання, що супроводжується процедурою банкрутства, дуже непросто. Насамперед тому, що вся процедура банкрутства, як правило, від початку до кінця курирується одним суддею. Якщо він діє в інтересах поглинача, що поглинає компанії прийде туго.

Крім того, у незадоволеної сторони немає підстав подавати апеляції. Справа в тому, що визначення про порушення справи про банкрутство не може бути предметом оскарження, тому що формально воно не є рішенням суду. Украй рідко, посилаючись на Конституцію, вдається заперечити таке визначення.

Можна заперечувати призначення арбітражного керуючого, але часто судді призначають його відразу, одночасно з відкриттям справи про банкрутство. Згодом повинне з'явитися рішення судді про початок ліквідаційної процедури, що також можна заперечувати, але до цього

пройде чимало часу, протягом якого власник, як правило, уже губить контроль над підприємством.

Якщо у звичайних господарських суперечках є рішення суду, виконання якого можна зупинити подачею апеляції, то справа про банкрутство зупинити не можна. Зате по ходу справи можна заявити відвід арбітражному керуючий, а кожної із кредиторів має право заперечити його дії в суді.

Відслідковуючи рух векселів можна підстрахуватися від виникнення фіктивних боргів і надуманого банкрутства. Крім того, у договорах з контрагентами має сенс передбачити заборону передачі боргів третім особам або обов'язкове повідомлення про це - у такому випадку початок процедури банкрутства можна заперечувати, посилаючись на незаконність придбання боргу.

Скупка акцій

Знизити ризик недружнього поглинання можна постійним моніторингом угод по акціях підприємства. Для цього потрібно регулярно звертатися до реєстратора й відслідковувати всі угоди по акціях. Якщо раптово кількість угод зростає на порядок, цілком можливо, хтось організував скупку з метою поглинання. У цьому випадку для збереження незалежності менеджменту іноді доводиться скуповувати акції свого підприємства, намагаючись зібрати необхідний для цього пакет (75%+1 акція), а після, шляхом додаткової емісії, намагатися знецінити скуплені конкурентами акції.

Щоб власники Відкритого акціонерного товариства (ВАТ), були абсолютно спокійні за долю компанії, їм потрібно володіти мінімум 76% підприємства. У такому випадку недружній поглинач втрачає можливості легально придбати контроль над підприємством - він може лише спробувати ініціювати процедуру банкрутства по наведеним вище сценаріях.

Також доцільно із числа акціонерів створити наглядацька рада, що буде контролювати дії керуючого компанією, що мінімізує можливість зловживань із його боку. З погляду можливостей захисту від поглинання, закрите акціонерне товариство перебуває в більше вигідному положенні, чим відкрите, оскільки при продажі цінних паперів кожен акціонер зобов'язаний запропонувати їх спочатку іншим власникам, для чого необхідно скликати збори акціонерів.

Акції закритого акціонерного товариства (ЗАТ), у вільний продаж надходять лише після того, як всі інші акціонери компанії офіційно відмо-

вилися від їхнього придбання. Таким чином, недружнє поглинання ЗАТ шляхом скупки акцій значно ускладнюється.

Ефективним способом захисту відкритого акціонерного товариства від поглинання може бути внесок його активів в інше підприємство. Звичайно після внеску активів акціонерне товариство реорганізовують у ТОВ, а колишні акціонери стають засновниками.

Думка експертів з цього приводу

Іноді після відмови власника продати підприємство поглиначі ініціюють цілий ряд перевірок при участі прокуратури, органів МВС, податкової інспекції. Як правило, що перевіряючи потім порушують кримінальну справу по факті якогось порушення. Справа, заведена по факту, не має чітких процесуальних строків розслідування, його можна вести нескінченно довго, періодично допитуючи ключових співробітників і керівників компанії як свідків, вилучаючи первинні бухгалтерські документи й заарештовуючи рахунку. Все це приводить до збоїв у роботі підприємства, затримці розрахунків з контрагентами й нагромадженню боргів. До речі, вилучені бухгалтерські документи підприємству не повертають, тому що вони стають доказами в кримінальній справі. А працювати не маючи первинної документації, проблематично.

Гірше всього, коли перевірка проводиться законно - і що у перевіряючих є службові посвідчення, розпорядження на перевірку, постанову про порушення кримінальної справи.

Після цього загарбник цілком обґрунтовано припускає, що підприємство буде йому продано, тому що власникам не захочеться зазнавати збитків і вони будуть згодні на продажу. Багато підприємств на цьому етапі продаються, навіть якщо поглинач пропонує не занадто високу ціну.

Соціальний захист

На одному досить привабливому заводі у Львівській області раптово почався шквал перевірок. Керівництву було видно, що перевіряючі діють у чиїхось інтересах. Але ініціатор ніяк себе не проявляв. При розвитку подій по силовому сценарії, установити, хто це організував, практично неможливо до появи покупця.

У цьому випадку власники не здавалися, з юристами скаржилися в усі інстанції на незаконні дії працівників що перевіряють, оскаржили рішення контролюючих органів. Коли поглинач побачив настільки розпачливий опір власників, він перейшов до іншого варіанта дій - почав ску-

повувати борги заводу. А боргів через різний рід затримок нагромадилося досить багато.

Крім того, підприємство не платило в соціальні фонди через арешт рахунків. Після скупки боргів була досягнута певна домовленість із Пенсійним фондом і всіма соціальними фондами про координацію дій. Покупець попередив їх про процедуру, що почалася, банкрутства заводу, і запропонував їм виплати заборгованості, що вони й зробили. У підсумку підприємство було признано банкротом а його активи були викуплені поглиначем. Завод перейшов до іншого власника

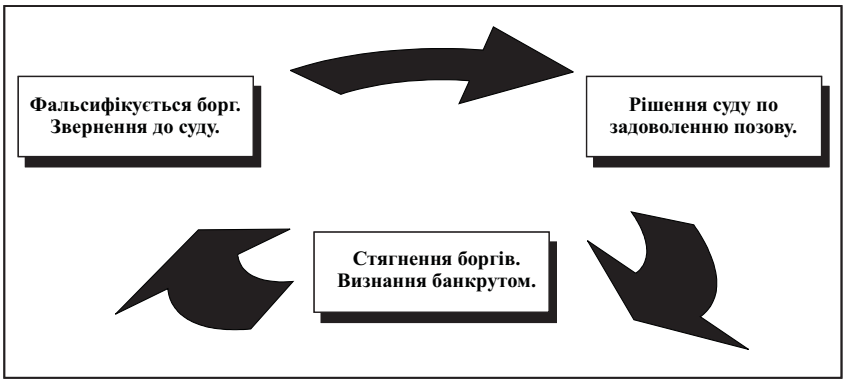
Схема поглинання компанії шляхом банкрутства

1.) Поглинач здобуває або фальсифікує борг підприємства

Суть явища: поглинач одержує підстави звертатися в суд з вимогою стягнути з підприємства-жертви заборгованість

2.) Поглинач звертається в суд з позовом про стягнення з підприємства заборгованості. Суд задовольняє позов, постановляючи стягнути з підприємства заборгованість й оплатити судові витрати

Суть явища: при цьому поглинач намагається, щоб підприємство-жертва не знало про початок судового виробництва й не одержало рішення суду. Також нападаючий !намагається досягти домовленості зі співробітниками державної виконавчої служби, щоб з підприємства, що поглинає, не був стягнений борг виконавцями



3.) По закінченні трьох місяців, якщо рішення суду про примусове стягнення боргу не було виконано, поглинач звертається в суд з позовом про визнання боржника банкрутом. Суд задовольняє позов, виносячи ви-

значення про початок процедури банкрутства, призначаючи арбітражного керуючого

Суть явища: за допомогою підконтрольний арбітражний керуючий поглинач одержує можливість утрудняти або блокувати нормальну роботу підприємства-жертви.

6.3. Зовнішні джерела погроз діяльності підприємства

Щодо питань несумлінної конкуренції підприємництва, то тут ще необхідна серйозна як теоретична, так і організаційно-практична робота з питань утворення певної організаційно-правової інфраструктури безпеки. Слід відзначити, що виявляти ризики та порушення, які посягають на загальну безпеку підприємництва, в силу їх природи і процесуально-правової структури, в більшості випадків покладені на не державні спецслужби тих суб'єктів підприємництва, яким завдаються збитки. Така стратегія базується на тому, що ризики економічних та інших зловживань на перший погляд, як правило, знаходяться у сфері дії цивільно-правових норм. Мотивом такої роботи є запобігання збитків від різного роду ризиків та посягань.

В умовах, що склалися, тільки такий підхід дозволяє підприємцям, банкірам, страховикам забезпечити надійний захист як від прорахунків щодо неефективного вкладення і використання коштів, несумлінної конкуренції, так і від різноманітних правопорушень, у тому числі і криміногенного характеру. Як бачимо з характеру цих діянь, до проблем детінізації природним шляхом залучається ціла "армія" службових підрозділів підприємницької безпеки. Як ефективніше їх використати – залежить від того, чи зможе держава створити комплексну організаційно-правову інфраструктуру, в межах якої будуть вирішуватись питання детінізації економіки.

Хоча попередження зазначених протиправних посягань на майно підприємств уже відіграє певну роль в оздоровленні оперативної обстановки, а відповідно і в питаннях детінізації економіки.

Питання безпеки підприємництва тісно пов'язане з підприємницькими, фінансовими, кредитними, страховими та іншими ризиками, що супроводжують фінансово-господарську діяльність.

Саме підприємництво, його фінансово-кредитне обслуговування, страхування кредитних, підприємницьких та інших ризиків є невід'ємними, тісно пов'язаними елементами успішного функціонування економіки.

Оскільки підприємництво на сучасному рівні розвитку практично не може існувати без кредитів, тому на основі опрацювання систем і засобів управління кредитними, страховими та іншими ризиками, пов'язаними з ними, можна побудувати інфраструктуру економічної безпеки не тільки у сфері банківської діяльності, а й підприємництві в цілому, що безумовно впливає і на питання детінізації економіки. Саме кредитні і страхові ризики найчастіше займають центральне місце серед інших видів ризиків, що впливають на економічну безпеку підприємництва.

Тому, маючи на меті розробку ключових алгоритмів системи економічної безпеки у сфері підприємництва, доцільно розглянути основні інститути цієї системи, а саме:

1) - внутрібанківські засоби та системи економічної безпеки у сфері кредитних відносин;

2) - організаційно-правові форми, структуру та принципи страхової справи як фактора зниження ризиків у сфері підприємництва;

3) - інші види гарантій щодо зниження ризиків у сфері фінансово-господарської діяльності;

4) - захист інформації з обмеженим доступом, її правовий режим.

Слід підкреслити, що комплексна система економічної безпеки підприємництва передбачає більш широке коло систем і засобів управління підприємницькими ризиками, особливо коли йдеться про створення цілісної інфраструктури економічної безпеки у сфері підприємницької діяльності. …Розгляд цієї проблеми через призму запропонованих ключових інститутів системи економічної безпеки дає змогу вийти на алгоритми створення економічних фінансових, інформаційно-аналітичних, організаційних та правових систем управління ризиками у сфері підприємництва, а відповідно і перманентного впливу на проблеми детінізації економіки. Наприклад, проблеми, що виникають у кредитних відносинах на сучасному рівні господарювання, мають вирішальний характер.

В умовах первинного накопичення капіталів кредит є інструментом, без якого підприємництво і особливо функціонування товарного виробництва неможливо взагалі. У зв'язку з цим доцільно відзначити, що, коли в країні кредитний обіг набуває стихійного характеру, кризи в економіці не уникнути. Це стосується економіки з будь-якою формою власності.

Згадаємо, що антикризова програма Президента США Ф. Рузвельта у роки великої депресії (30-ті роки) базувались на заходах упорядкування кредитно-фінансових відносин. Від ефективності і безперебійності функціонування кредитно-фінансового механізму залежить не тільки своєчасне одержання фінансових засобів функціонування окремими підприємницькими структурами, а й економічний розвиток країни. Зловживання й інші негативні тенденції, що виникають у фінансово-кредитній системі і економіці в цілому, вимагають зваженого підходу і скоординованої роботи підприємців, банків і страхових компаній.

Саме загальний інтерес згаданих суб'єктів підприємницької діяльності є стимулом для забезпечення життєдіяльності один одного, а паралельно може позитивно впливати на питання детінізації економіки. Цей спільний інтерес і є центральною ланкою, яка визначає ключові позиції структури управління фінансовими ризиками у банківській діяльності, страхуванні, гарантійному забезпеченні зниження ризиків тіньових процесів у підприємництві в цілому.

Стрижневими напрямками проти дії несумлінній конкуренції - є також проблеми щодо захисту інформації з обмеженим доступом. Вона стосується будь-якого напряму підприємницької діяльності як у сфері виробництва, так і у сфері послуг чи інших напрямах підприємництва.

Замахи на конфіденційну інформацію

Перш ніж розпочати розгляд проблем взаємодії учасників фінансово-господарських відносин між собою та з відповідними державними органами, визначимо категорії інформації з режимом обмеженого доступу та деякі концептуальні аспекти, що заважають гармонізації інформаційних відносин та розв'язанню проблем економічної безпеки у сфері підприємництва.

В протидіях несумлінній конкуренції насамперед необхідно визначити те, що:

1. Права і обов'язки власників інформації з обмеженим доступом, а також організацій, яким така інформація повинна надаватися, в існуючих

правових нормах розглядаються окремо, хоча за своєю природою вони є взаємопов'язаними.

2. Підстави віднесення інформації до категорій з обмеженим доступом у Законі "Про інформацію" визначені нечітко, правове поле інформаційних відносин не має механізму взаємного зв'язку між користувачами і не стимулює утворення системи економічної безпеки учасників фінансово-господарських відносин, з одного боку, і не утворює комплексної організаційно-правової інфраструктури детінізації економіки – з іншого.

3. Структура і зміст ринкових відносин, що базуються на конкуренції між суб'єктами підприємництва, ускладнюють проблему взаємного обміну інформацією.

4. Оскільки метою інститутів банківської і комерційної таємниці є передусім встановлення режиму безпечної діяльності учасників підприємницьких відносин, то подолання суперечностей у питаннях їх взаємодії можна вирішити тільки шляхом комплексного підходу при опрацюванні нормативної бази, що регулює доступ до тієї чи іншої категорії інформації, а також через утворення спільної системи колективної економічної безпеки для всіх суб'єктів підприємницької діяльності.

Разом із тим, конкретизувати ці питання можливо тільки після детального правового аналізу відповідної нормативної бази, що лежить в основі визначення категорій закритої інформації, а також аналізу порядку надання такої інформації та гарантій її законного використання.

Чинним законодавством визначені **три категорії інформації з обмеженим доступом** до неї:

– інформація, що складає банківську таємницю;

– інформація, що містить комерційну таємницю;

– конфіденційна інформація.

1.) Щодо першої категорії інформації, Закон України від 20.03.91 "Про банки і банківську діяльність" не дає визначення банківської таємниці. Проте, виходячи з редакції ст. 52, банківську таємницю складають відомості про операції, рахунки і вклади клієнтів, а також кореспондентів банків.

2.) Поняття комерційної таємниці дано в ст. 30 Закону України від 27.03.91 "Про підприємства в Україні": "Під комерційною таємницею підприємства маються на увазі відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам".

Стаття 1 цього Закону визначає: "Підприємництво – самостійний господарюючий статутний суб'єкт, який має права юридичної особи та здійснює виробничу, науково-дослідницьку і комерційну діяльність з метою одержання відповідного прибутку (доходу)". Виходячи з наведеного визначення, до числа підприємств у цьому розумінні можна віднести і комерційні банки.

3.) Відповідно до ст. 30 Закону України "Про інформацію", конфіденційна інформація за своїм правовим режимом належить до інформації з обмеженим доступом. Її складають "...відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов".

Як бачимо, Закон не дає визначення інформації, що становить комерційну таємницю чи є конфіденційною, а замість цього надає необмежені права її власникам у частині встановлення переліку відповідних відомостей.

У зв'язку з цим, як один із прикладів, розглянемо, які відомості до числа таких, що складають комерційну і конфіденційну таємницю (за змістом наведених нами статей Закону "Про підприємства в Україні" і Закону "Про інформацію"), на практиці відносять банківські установи.

Відомості, що складають комерційну таємницю:

1. Відомості про принципи управління банком:

- про підготовку, прийняття і виконання окремих рішень керівництва банку з усіх нижчеперелічених питань;
- про перспективні плани і методи управління банком;
- про факти підготовки, мету і проведення ділових переговорів, про предмет і цілі нарад, засідання органів управління банку;
- документація управління, ради банку, загальних зборів акціонерів;
- відомості і документи, що стосується питань ділової політики банку.

2. Відомості про фінансову діяльність банку:

- ті, що розкривають планові і фактичні показники фінансового плану;
- бюджет банку;
- майновий стан банку;
- про обіг банківських коштів;
- про рівень прибутку банку;
- про банківські операції;
- про фінансові операції банку;
- про специфіку міжнародних розрахунків з іншими банками;
- про планові та звітні дані за валютними операціями;
- про стан рахунків клієнтів банку і операції, що по них проводяться;
- про величину активних і пасивних операцій;
- про джерела кредитних ресурсів банку;
- про стратегію і тактику з валютних і кредитних питань;
- про методи розрахунків, структуру і розмір знижок;
- про кредитні та валютні відносини з іноземними банками і фірмами;
- про умови за договорами (контрактами);
- про умови платежів за контрактами;
- матеріали аудиторських перевірок і ревізій банку та його філій;

- про порядок користування печаткою і штампами банку;
- відомості про порядок оформлення гарантій банку.

3. Відомості у сфері програмного забезпечення банку:

- комп'ютерні програми, що використовуються в роботі банку і його філій;
- ті, що зберігаються на магнітних носіях в електронно-обчислювальних машинах банку;
- про паролі і коди, що використовуються допущеними до цієї роботи службовцями банку при входженні у банківські комп'ютерні мережі.

4. Відомості про клієнтів і партнерів банку:

- систематизовані відомості про клієнтів банку і його контрагентів за договорами;
- про відносини банку з іноземними партнерами.

5. Інші відомості:

- про порядок і стан організації захисту комерційної таємниці і конфіденційної інформації банку;
- про порядок і стан організації охорони і пропускного режиму, систему сигналізації;
- ті, що складають комерційну таємницю чи конфіденційну інформацію клієнтів і контрагентів банку;
- інформація служби безпеки банку.

Тепер розглянемо перелік відомостей, що належать до конфіденційної інформації:

1. Відомості про персонал банку:

- ті, що знаходяться в особових справах службовців банку;
- про зміни в кадровій політиці банку, що плануються;
- про чисельність і склад службовців, про фонд їх заробітної плати, а також про наявність вакантних робочих місць.

2. Відомості про систему матеріально-технічного забезпечення банку:

- про транспортні й енергетичні потреби банку;
- про маршрути і цілі поїздок банківського транспорту;
- про розміщення складських і підсобних приміщень, режим надходження цінностей, устаткування тощо, а також про систему їх охорони.

Конфлікт інтересів між правомірним користувачем і власником інформації (на прикладі банківських установ)

Конфлікт інтересів між правомірним користувачем і власником інформації знижує ефективність заходів локалізації джерел підпільного (криміногенного) сектора тіньової економіки і не створює конкретної організаційно-правової інфраструктури детінізації економіки. Розмежовуючи поняття банківської, комерційної таємниці та конфіденційної інформації, законодавець встановлює різний правовий режим її використання.

Основоположний для банків Закон України "Про банки і банківську діяльність" дає відносно повний перелік інформації, що складає банківську таємницю, а також тих органів і організацій, яким вона може бути передана.

Відповідно до ст. 52 цього Закону "довідки про операції і рахунки юридичних осіб та інших організацій видаються самим організаціям, державним податковим інспекціям з питань оподаткування, а також у випадках, передбачених законодавством, на письмову вимогу судам, органам прокуратури, служби безпеки, внутрішніх справ, Антимонопольного комітету України, державної контрольно-ревізійної служби, арбітражному суду та аудиторським організаціям.

Довідки про рахунки і вклади громадян видаються, крім самих клієнтів та їх представників, також судам, органам прокуратури, служби безпеки, внутрішніх справ у справах, що знаходяться в їх провадженні".

Протиріччя і суперечності відповідно до основних Законів України.

У ході аналізу наведених норм Закону потрібно звернути увагу на такі суперечності.

Державним податковим інспекціям можуть видаватися лише довідки про операції і рахунки юридичних осіб та інших організацій. Надання їм інформації по рахунках і вкладах громадян законодавець не згадує. У переліку органів і організацій, яким видаються довідки про рахунки і вклади громадян, відсутні також арбітражний суд, органи державної контрольно-ревізійної служби, аудиторські організації, хоча нормативні акти, що регулюють їх діяльність, надають їм право звертатися до банку з питань видачі їм такої інформації.

Якщо для одержання інформації про рахунка і вклади громадян обов'язковою є наявність у провадженні правоохоронного органу відповідної справи, то для одержання довідки про операції і рахунки організацій ця умова не передбачається, однак робиться застереження про

те, що відомості можуть бути надані лише у випадках, передбачених законодавством.

Практично нічого не згадується в законі про порядок надання банками відомостей один одному та іншим суб'єктам підприємництва. Між іншим, обмін інформацією між банками вкрай необхідний для зниження ризику неповернення кредитів, оскільки за кредитом юридичні особи-позичальники звертаються найчастіше всього в такий банк, де їх платоспроможність та імідж можуть бути невідомі. Аналогічна ситуація існує при наданні комерційних кредитів, коли підприємства передають товари, надають послуги під вексель з відстрочкою платежу чи роблять передоплату з відстрочкою одержання товарів і виконання послуг.

Ще більше протиріч у правовому регулюванні режиму комерційної таємниці. У пункті 2 ст. 30 Закону України "Про підприємства в Україні" визначено: "Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства".

Виняток (відповідно до Закону України "Про інформацію") складають відомості, правовий режим яких встановлюється Верховною Радою України. Слід відзначити, що будь-які винятки, не вказані чітко в законі, і такі, що не враховують всю нормативну інфраструктуру правового регулювання конкретного питання (в тому числі і безмежні права власника інформації, зазначені у статтях 30 Законів "Про інформацію" і "Про підприємства"), не тільки створюють серйозні суперечності в питаннях забезпечення захисту конфіденційної інформації, але й знижують економічну безпеку (через відсутність інформації про надійність позичальника кредитів чи партнерів з інших видів угод). У цьому зв'язку слід ще раз відзначити, що відносини між суб'єктами підприємництва з приводу обміну інформацією про надійність партнерів за фінансово-господарськими угодами закон майже не регулює. Можливе лише тлумачення тієї чи іншої норми стосовно конкретної ситуації. Але при такому підході комплексний і ефективний механізм взаємодії та обміну інформацією створений бути не може.

Інші суперечності нормативної бази

Суттєві суперечності має нормативна база, що регулює надання тих чи інших відомостей правоохоронним, судовим та іншим контролюючим органам. Наприклад, інформаційні відносини банків з органами внутрішніх справ, крім Закону "Про банки і банківську діяльність", регу-

люють ще п'ять нормативних актів, а відповідно і ст. 22 Закону України "Про внесення змін до Закону України "Про державну податкову службу в Україні", і органами податкової міліції.

Відповідно до п. 17 ст. 11 Закону України "Про міліцію" органам міліції надається право: "одержувати безперешкодно і безплатно від підприємств, установ і організацій незалежно від форм власності та об'єднань громадян на письмовий запит відомості (у тому числі й ті, що становлять комерційну та банківську таємниці), необхідні у справах про злочини, що знаходяться у провадженні міліції".

Ця норма кореспондується з положеннями Закону "Про банки і банківську діяльність" і коментарю не потребує. В інших нормативних актах права органів внутрішніх справ на одержання закритої інформації трактуються суперечливо, що не сприяє виконанню ними своїх службових обов'язків.

Так, у п. 5 Положення про Державну службу боротьби з економічною злочинністю, затвердженого постановою Кабінету Міністрів України від 05.07.93 № 510, вказано, що працівники цієї служби "... при наявності даних про порушення законодавства, що регулює фінансову, господарську та іншу підприємницьку діяльність, які тягнуть за собою кримінальну відповідальність...", мають право:

* пп. 3 – "вилучати необхідні матеріали про кредитні та фінансові операції... у встановленому законодавством порядку";
* пп. 7 – "одержувати безкоштовно від підприємств, установ, організацій і громадян інформацію, за винятком випадків, коли законом встановлений спеціальний порядок її одержання";
* п. 11 – "одержувати в установленому порядку від Національного банку та його установ, комерційних банків та інших кредитних установ необхідні відомості, копії документів, довідки про банківські операції і залишки коштів на рахунках об'єктів, що перевіряються...".

Із редакції ст. 5 Положення витікає, що викладених досить широких прав зазначена служба МВС набуває незалежно від того, порушено кримінальну справу чи ні, з моменту одержання даних про правопорушення. Проте слід мати на увазі, що в усіх трьох наведених пунктах цієї статті міститься застереження про те, що дані права реалізуються у встановленому законодавством порядку або коли законом установлено спеціальний порядок одержання інформації.

Такий порядок визначений Законами "Про банки і банківську діяльність" і "Про міліцію", де вказано, що конфіденційна інформація може бути передана тільки при наявності справи і за письмовим запитом. Відомо, що в разі розбіжностей у правових нормах повинен спрацьовувати принцип верховенства закону над підзаконним актом. Таким чином, "широкі" права цієї служби зводяться нанівець, оскільки під "справою" власники інформації розуміють кримінальну справу, але, перш ніж порушити її, необхідно мати не тільки оперативну інформацію, а й конкретні документи. Останні ж можна одержати після порушення кримінальної справи. Створюється замкнуте коло.

Відповідно до ст. 12 Закону України "Про організаційно - правові основи боротьби з організованою злочинністю" підрозділам з боротьби із такими проявами надаються повноваження:

* – п. 2 "б" – "на письмову вимогу керівників відповідних спеціальних підрозділів з боротьби із організованою злочинністю одержувати від банків, а також кредитних, митних, фінансових та інших установ, підприємств, організацій (незалежно від форм власності) інформацію і документи про операції, рахунки, вклади, внутрішні та зовнішні економічні угоди фізичних і юридичних осіб. Документи та інформація повинні бути надані негайно, а якщо це неможливо – не пізніше ніж протягом 10 діб";

* – п. 2 "д" – "у разі одержання фактичних даних про організовану злочинну діяльність для їх перевірки витребувати та одержувати від... підприємств, установ, організацій (незалежно від форм власності) інформацію і документи. Витребувані документи та інформація повинні бути надані негайно або не пізніше ніж протягом 10 діб".

Наведені норми дещо відрізняються від викладених раніше. Слід звернути увагу на те, що тут не ставиться умова наявності справи. Більше того, у п. 2 "д" вказано, що підрозділи з боротьби із організованою злочинністю набувають право витребувати конфіденційну інформацію "при одержанні фактичних даних про організовану злочинну діяльність". Поряд із цим, жоден законодавчий акт не дає поняття "фактичні дані".

Крім того, існують суперечності між положеннями статті 12 Закону, що аналізується, і положеннями статті 33 Закону України "Про інформацію", у якій вказується: "Термін вивчення запиту на предмет можливості його задоволення не повинен перевищувати десяти календарних днів. Протягом вказаного терміну державна установа письмово дово-

дить до відома запитувача, що його запит буде задоволено або що запитуваний документ не підлягає наданню для ознайомлення.

Задоволення запиту здійснюється протягом місяця, якщо інше не передбачено законом". Відповідно до ст. 8 Закону України "Про оперативно-розшукову діяльність" оперативним підрозділам органів внутрішніх справ (як і інших правоохоронних органів) при наявності до того підстав надається право:

- п. 4 – "витребувати, збирати і вивчати документи і дані, що характеризують діяльність підприємств, закладів, організацій, а також спосіб життя окремих осіб, які підозрюються в підготовці та вчиненні злочину, джерело і розміри їх прибутку";
- п. 14 – "одержувати від юридичних і фізичних осіб безкоштовно чи за винагороду інформацію про злочини, що готуються, або скоєні злочини і загрозу безпеці суспільства і держави"'.

Самі по собі ці права ніяких сумнівів у їх правомірності і необхідності не викликають. Питання лише в тому, які підстави породжують зазначені права. У статті 6 цього ж Закону до переліку підстав для проведення оперативно-розшукової діяльності (у тому числі і витребування необхідних відомостей) включені:

- п. 1 – наявність достатньої інформації про:

а) злочини, які готуються або вчинені невстановленими особами;

б) осіб, які готують або які вчинили злочин;

в) осіб, які переховуються від органів розслідування чи які ухиляються від відбування кримінального покарання;

г) осіб, які пропали безвісти;

д) розвідувально-підривну діяльність спецслужб іноземних держав, організацій і окремих осіб проти України;

- п. 2 – запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної, військової та службової таємниці;
- п. 3 – потреба в одержанні розвідувальної інформації в інтересах безпеки суспільства і держави.

Відповідно до статті 66 Кримінально-процесуального кодексу України: "Особа, яка провадить дізнання, слідчий, у тому числі і податкової міліції, прокурор і суд у справах, які знаходяться в їх провадженні, мають право... вимагати від підприємств, установ, організацій, по-

садових осіб і громадян пред'явлення предметів і документів, які можуть встановити необхідні у справі фактичні дані... Виконання цих вимог є обов'язковим для всіх громадян, підприємств, установ і організацій".

Щодо аналізу наведених витягів із законодавчих актів, слід відзначити такі обставини:

- **по-перше** – закон надає право витребування відомостей і документів за кримінальними справами;
- **по-друге** – просто за справами, що знаходяться у провадженні;
- **по-третє** – при наявності інформації про злочини;
- **по-четверте** – при наявності потреби одержання розвідувальної інформації в інтересах держави і суспільства.

Статус усіх перелічених підстав доступу правоохоронних органів до інформації, що містить банківську, комерційну таємницю та інші конфіденційні відомості, не тільки суперечливий, але й обумовлює цілком різні процесуальні дії відповідних посадових осіб, детермінує конфліктну ситуацію між ними і власниками цієї інформації. Така розбіжність щодо підстав для витребування інформації не може сприяти ні боротьбі зі злочинністю, ні захисту банківської і комерційної таємниць, ні підвищенню рівня економічної безпеки суб'єктів підприємництва в процесі здійснення фінансово-господарської діяльності.

Причини: **По-перше**, всі ці норми опрацьовувалися в різний час і в різних соціально-економічних і політичних умовах. **По-друге**, розробники деяких актів намагалися вирішити якісь вузьковідомчі поточні завдання без урахування інтересів усіх учасників, які працюють у полі інформаційних відносин.

Розв'язати зазначені суперечності можна тільки при комплексному підході до даної проблеми, ставлячи перед собою основне завдання – утворення ефективного механізму економічної безпеки всіх учасників інформаційно-правового простору у сфері фінансово-господарських відносин, у тому числі і держави.

Те ж саме можна сказати з приводу термінів надання документів. Вони коливаються від "негайно", "десять днів" і до місяця. При цьому обґрунтування, від чого такі терміни залежать (від кількості запитуваних документів чи ще якихось чинників), не дається.

Інформаційні взаємовідносини між суб'єктами

Інформаційні відносини банків з органами служби безпеки, як і з органами внутрішніх справ, регулюються великою кількістю нормативних актів. Крім Законів, що уже згадувалися ("Про інформацію", "Про банки і банківську діяльність", "Про оперативно-розшукову діяльність", "Організаційно-правові основи боротьби з організованою злочинністю" і ст. 66 КПК України), повноваження органів служби безпеки щодо витребування конфіденційної інформації закріплені в ст. 25 Закону України "Про службу безпеки України", де вказано, що її органи і співробітники мають право: "одержувати на письмовий запит керівника відповідного органу... від підприємств, установ, організацій дані та відомості, необхідні для забезпечення державної безпеки України, а також користуватися з цією метою службовими документами і звітністю". Тут закладені всі перелічені вище суперечності. Причини їх ті ж.

Повноваження органів прокуратури, викладені у ст. 66 КПК України, вже наводилися. Вони також відображені у ст. 20 Закону України "Про прокуратуру", де вказано, що при здійсненні нагляду прокурор має право:

* п. 1 – "... мати доступ до документів і матеріалів, необхідних для проведення перевірки, в тому числі за письмовою вимогою й тих, що містять комерційну чи банківську таємниці або конфіденційну інформацію. Письмово вимагати надання в прокуратуру для перевірки зазначених документів та матеріалів, видачі необхідних довідок, у тому числі про операції і рахунки юридичних осіб та інших організацій, для вирішення питань, пов'язаних з перевіркою";

*п. 2 – "вимагати для перевірки рішення, розпорядження, інструкції накази та інші акти і документи, одержувати інформацію про стан законності і заходи щодо її забезпечення".

Відповідно до ст. 8 цього Закону "вимоги прокурора, які відповідають чинному законодавству, є обов'язковими для всіх органів, підприємств, установ, організацій, посадових осіб та громадян і виконуються невідкладно або у передбачені законом чи визначені прокурором строки". У Законах "Про інформацію", "Про банки і банківську діяльність" та інших про такі повноваження не згадується. Оскільки закони за своїм статусом рівні, то прокурор виконує вимоги "свого закону", а банкір – "свого". Виграє той, хто наполегливіший. Але це знаходиться дуже далеко від так званих "цивілізованих" і тим більш правових відносин.

Правовідносини сторін

Заслуговує на увагу нормативне регулювання прав суду. Наведений вище правовий аналіз ст. 66 КПК України був би неповним без урахування положень ст. ст. 47 і 143 Цивільно-процесуального кодексу України.

Відповідно до ст. 143 ЦПК України при підготовці справи до судового розгляду суддя "вимагає від державних підприємств, установ, організацій, колгоспів, інших кооперативних організацій, їх об'єднань, інших громадських організацій, а також від громадян письмові і речові докази або надає особам, які беруть участь у справі, повноваження на право одержання цих доказів для подачі їх до суду..."

У ст. 47 ЦПК України зазначено, що "письмові докази, що витребувалися судом чи суддею від державних підприємств, установ, організацій.., направляються безпосередньо до суду".

Суд або суддя може також уповноважити зацікавлену сторону чи іншу особу, яка бере участь у справі, одержати письмовий доказ для представлення його суду".

Таким чином, якщо під установами чи підприємствами розуміти і банки, то вони зобов'язані надавати на вимогу суду документи та інформацію як самому суду, так і уповноваженим ним особам, що не узгоджується з Законом України "Про банки і банківську діяльність".

Норми інших законодавчих актів

Для більш повної картини стану нормативного регулювання інформаційних відносин між банками, установами та організаціями слід навести окремі норми, що містяться і в інших законодавчих актах.

Ст. 10 Закону України "Про Державну контрольно-ревізійну службу в Україні" надає право відповідним органам "одержувати від Національного банку України та його установ, комерційних банків та інших кредитних установ необхідні відомості, копії документів, довідки про банківські операції та залишки коштів на рахунках об'єктів, що ревізуються або перевіряються..."

У ст. 65 Арбітражного процесуального кодексу України зазначається, що при підготовці справи до розгляду арбітр "зобов'язує сторони, інші підприємства, установи, організації, державні та інші органи, їх посадових осіб виконати певні дії (звірити розрахунки, провести огляд доказів у місці їх знаходження тощо); витребовує від них документи, відомості, висновки, необхідні для вирішення спору, чи знайомиться з такими матеріалами безпосередньо в місці їх знаходження".

Закон України “Про адвокатуру” у ст. 6 надає адвокатові право “збирати відомості про факти, які можуть бути використані як докази у цивільних, господарських, кримінальних справах і справах про адміністративні правопорушення, зокрема:

- – запитувати і отримувати документи чи їх копії від підприємств, установ, організацій, об’єднань...;
- – ознайомлюватись на підприємствах, в установах і організаціях із необхідними для виконання доручення документами і матеріалами, за винятком тих, таємниця яких охороняється законом”.

Відповідно до статті 4 Закону України “Про нотаріат” нотаріус має право “витребувати від підприємств, установ і організацій відомості і документи, необхідні для вчинення нотаріальних дій”. Відповідно до Указу Президента України від 18.06.93 № 218/93 “Про Координаційний комітет з питань боротьби зі злочинністю” цьому комітету надані права (ст. 3):

- – доручати відповідним державним органам чи створюваним Координаційним комітетом комісіям проведення перевірок додержання органами державної виконавчої влади, підприємствами, установами і організаціями усіх форм власності фінансово-кредитної дисципліни, встановленого порядку бухгалтерського обліку, сплати податків та внесення інших платежів до бюджету;
- – ...вимагати від... підприємств, установ, організацій усіх форм власності інформацію щодо виконання ними рішень і рекомендацій Координаційного комітету;
- – ...безперешкодного відвідування (як членами Координаційного комітету, так і уповноваженими ним особами) підприємств, установ і організацій усіх форм власності, знайомитися в установленому порядку і в межах своїх повноважень з відповідними документами”.Відповідно до ст. 2 Закону України “Про аудиторську діяльність” аудиторські фірми і аудитори мають право:
- – п. 2 – “отримувати необхідні документи, які мають відношення до предмета перевірки і знаходяться як у замовника, так і у третіх осіб.

Треті особи, що мають у своєму розпорядженні документи стосовно предмета перевірки, зобов’язані надати їх на вимогу аудитора (аудиторської фірми). Зазначена вимога повинна бути офіційно засвідчена замовником”.

Права Національного банку України визначені Законом України "Про банки і банківську діяльність"

У ст. 16 Закону вказано, що "Національний банк видає нормативні акти з питань, що входять до його повноважень. Нормативні акти Національного банку, прийняті в межах його повноважень, є обов'язковими для всіх юридичних та фізичних осіб і набирають чинності у визначений ним термін".

У ст. 48 Закону міститься таке положення: "Національний банк здійснює контроль за додержанням юридичними особами банківського законодавства та власних нормативних актів".

Відповідно до ст. 24 Закону України "Про страхування" у разі необхідності страховик може робити запити про відомості, пов'язані із страховим випадком, до правоохоронних органів, банків, медичних закладів та інших підприємств, установ і організацій, що володіють інформацією про обставини страхового випадку.

Підприємства, установи і організації зобов'язані надсилати відповідь страховикам на запит про відомості, пов'язані із страховим випадком, у тому числі й дані, що є комерційною таємницею. При цьому страховик несе відповідальність за їх розголошення в будь-якій формі, за винятком випадків, передбачених законодавством України.

Закон України "Про державну статистику" у ст. 10 надає органам державної статистики право "одержувати у встановленому порядку безкоштовно від усіх, на кого розповсюджується цей Закон, включаючи фінансові, банківські, митні та інші відомства і служби, і використовувати державну статистичну звітність та інші необхідні для проведення державних статистичних досліджень дані (на будь-якій стадії їх розробки), а також пояснення, що додаються до звітності".

Указом Президента України від 18.06.1993 р. № 219/93 "Про порядок виконання Державного бюджету України" Міністерству фінансів України надано право "одержувати від установ банків відомості щодо стану поточних бюджетних рахунків підприємств, організацій і установ".

У ст. 13 Закону України "Про ціни і ціноутворення" вказано, що "господарські суб'єкти повинні в установленому порядку подавати необхідну інформацію для здійснення контролю за правильністю встановлення і застосування цін".

Відповідно до Закону України "Про місцеві ради народних депутатів та місцеве і регіональне самоврядування" місцеві ради самоврядування мають право складати територіальні зведені фінансові баланси.

Відповідні державні і громадські органи, підприємства (об'єднання), організації і установи надають раді народних депутатів, її виконавчим і розпорядчим органам відомості, необхідні для їх складання.

У Законі України "Про зайнятість населення" у п. 2 ст. 19 сказано, що "державна служба зайнятості має право: одержувати від підприємств, установ і організацій, незалежно від форм власності, статистичні дані про наявність вакантних робочих місць, характер і умови праці на них, про всіх вивільнюваних, прийнятих і звільнених працівників та інформацію про передбачувані зміни в організації виробництва і праці, інші заходи, що можуть призвести до вивільнення працівників".

Відповідно до ст. 9 Закону України "Про зовнішньоекономічну діяльність" Міністерство зовнішньоекономічних зв'язків і торгівлі України здійснює контроль за додержанням усіма суб'єктами зовнішньоекономічної діяльності чинних законів України та умов міжнародних договорів України.

Відповідно до ст. 20 Закону України "Про охорону навколишнього природного середовища" до компетенції Міністерства охорони навколишнього природного середовища в Україні і його органів на місцях належить "... одержання безоплатно від міністерств, відомств, підприємств, установ та організацій інформації, необхідної для виконання покладених на нього завдань".

Закон України "Про обмеження монополізму і недопущення недобросовісної конкуренції в підприємницькій діяльності" встановлює (ст. 13), що "господарюючі суб'єкти (підприємці), органи влади і управління та їх службові особи зобов'язані на вимогу державних уповноважених, голів територіальних відділень Антимонопольного комітету України подавати документи, письмові та усні пояснення, іншу інформацію, необхідну для здійснення Антимонопольним комітетом України і його територіальними відділеннями завдань, передбачених чинним законодавством".

Загальний висновок і пропозиції

Необхідність надання всім переліченим органам інформації сумніву не викликає, оскільки без цього їх функціонування неможливе. Але, як бачимо, неузгодженість положень одного нормативного акта з положеннями іншого, як і в разі взаємовідносин органів внутрішніх справ із власниками відомостей, що складають банківську і комерційну таємниці, є й у взаємовідносинах останніх з іншими державними органами. Це істот-

но знижує ефективність їх роботи щодо протидії тінізації суспільно-економічних відносин, несумлінної конкуренції та інших посягань на безпеку підприємства.

Вихід із становища, що склалося, бачиться, передусім, в утворенні комплексної нормативної бази, яка регулює дані правовідносини (і не тільки стосовно правоохоронних органів), у створенні єдиного банку даних, в який відповідні органи, установи, організації в обов'язковому порядку і в установлені терміни надавали б точно визначені відомості, у тому числі конфіденційного характеру, і могли б у нормативно закріпленому порядку одержувати інформацію, відповідну завданням і повноваженням того чи іншого органу.

Без уваги не повинні залишитись і самі суб'єкти фінансово-господарських відносин, оскільки попередити заподіяння їм збитків, а відповідно і запобігти шахрайству або іншому корисливому злочину вони зможуть лише при отриманні інформації про імідж, платоспроможність і надійність свого партнера за фінансовою чи господарською угодою.

Створення такої комплексної інформаційно-аналітичної системи позитивно вплине на попередження зловживань між суб'єктами підприємницької діяльності, а відповідно на детінізацію економіки.

Розділ 7.

Контрольно-пропускний режим на підприємстві

Програмна анотація

7.1. Загальне значення контрольно-пропускного режиму підприємства.

7.2. Організація контрольно-пропускного режиму підприємства (КПР),

– розробка інструкцій по пропускному режимі,

– устаткування контрольно-пропускного пункту (КПП),

– пропуск співробітників та відвідувачів на об'єкт.

7.3. Забезпечення безпеки посадових і офіційних осіб,

– ініціативні і думаючі охоронці,

– проведення оцінки ваших охоронців,

– таємні служби США.

7.4. Газова зброя в умілих руках.

7.5. Бронежилет – як засіб індивідуального захисту.

7.6. Загальні міри по захисту від замаху,

– міри загальної безпеки при замахах.

7.1. Загальне значення контрольно-пропускного режиму

Побудова надійної системи безпеки, підприємства, фірми складний і багатогранний процес. Одним з немаловажних факторів забезпечення надійного захисту того або іншого об'єкта є організація й підтримка певного контрольно-пропускного режиму (КПР).

Контрольно-пропускний режим - це спеціальний режим організаційно-правових обмежень і правил, що встановлюють порядок пропуску через контрольно-пропускні пункти, в окремі будинки (приміщення) співробітників об'єкта, відвідувачів, транспорту й матеріальних засобів.

Основна мета контрольно-пропускного режиму - забезпечення нормативних, організаційних і матеріальних гарантій виявлення, попередження й припинення зазіхань на законні права підприємства, його майно, інтелектуальну власність, виробничу дисципліну й охоронювану інформацію.

Природне створення надійного контрольно-пропускного режиму вимагає знаних витрат. Однак, якщо уважно оцінити всі негативні фактори, впливу на діяльність фірми, ці витрати не здаються настільки великими, тому що забезпечують стійкий економічний рух фірми й зводять до мінімуму можливі втрати. До того ж процес створення системи контрольно-пропускного режиму може бути розтягнутий у часі, з урахуванням матеріальних можливостей фірми і її діяльності на ринку. Принципово важливою умовою для реалізації задуманого є аналіз ситуації й розробка програми дій, що дозволить уникнути торохкань і зайвих витрат.

Організація контрольно-пропускного режиму відрізняється певною складністю. Справа в тому, що механізм здійснення контрольно-пропускного режиму направлений на застосуванні "заборон" й "обмежень" у відношенні одних суб'єктів, що перетинають границі охоронюваних об'єктів, будинків (приміщень), для забезпечення прав й інтересів інших (фірми і її персоналу). Такий механізм регулювання правовідношення у сфері підприємництва повинен бути бездоганний з позиції вимог чинного законодавства.

У книзі ми будемо розглядати основні напрямки створення контрольно-пропускного режиму на підприємстві в загальному плані:

1.) методика визначення й оцінка вихідних даних;
2.) розробка заходів і нормативних документів;
3.) устаткування контрольно-пропускних пунктів;

7.2. Організація контрольно - пропускного режиму підприємства (КПР)

Контольно-пропускной режим є невід'ємною частиною загальної системи забезпечення безпеки фірми. Контольно-пропускной режим (як і вся система безпеки) повинен відповідати чинному законодавству, уставу фірми, підприємству, а також іншим нормативно-правовим актам, що регулюють діяльність організації.

1.) *Основні цілі* контольно-пропускного режиму зводяться до наступного:

- захист законних інтересів прав фірми, підтримка стійкості порядку внутрішнього керування;
- збереження власності фірми, її раціонального й ефективного використання;
- сприяти росту прибутків фірми;
- досягнення внутрішньої й зовнішньої стабільності підприємства;
- збереження комерційних секретів і прав інтелектуальну власність.

2.) **Вимоги** до організації контрольно-пропускного режиму підприємства:

- забезпечення санкціонованого проходу співробітників і відвідувачів, ввіз (вивіз) продукції й матеріальних цінностей, ритмічної роботи підприємства;
- виключати незаконний прохід осіб на охоронювані території й в окремі будинки (приміщення), безконтрольний в'їзд (виїзд) транспортних засобів;
- своєчасне виявлення погроз важливим інтересам фірми, причин й умов сприятливому нанесенню фірмі матеріального й морального збитку, її нормальному функціонуванню й розвитку;

- формування надійних гарантій підтримки організаційної стабільності зовнішніх і внутрішніх зв'язків фірми, відпрацьовування механізму оперативного реагування на погрози й негативні тенденції в розвитку;
- припинення зазіхань на законні інтереси фірми, використання юридичних, економічних, організаційних, соціально-психологічних, технічних й інших засобів у виявленні й ослабленні джерел погрози її безпеки.

3.) **Система забезпечення**. Контрольно-пропускний режим можна визначити як систему забезпечення нормативних, організаційних і матеріальних гарантій виявлення, попередження й припинення зазіхань на законні права підприємства, його майно, інтелектуальну власність, виробничу дисципліну, технологічне лідерство, наукові досягнення й охоронювану інформацію; сукупність організаційно-правових обмежень і правил пропуску, що встановлюють порядок, через контрольно-пропускні пункти співробітників об'єкта, відвідувачів, транспорту й матеріальних цінностей.

4.) **Нормативні гарантії** полягають у тлумаченні й реалізації норм права, з'ясування меж їхніх дій, у формуванні необхідних правовідносин, й забезпеченні правомірної діяльності підрозділів і працівників фірми із приводу її безпеки використання обмежувальних мір, застосуванням санкцій до фізичних й юридичних осіб, що зазіхають на законні інтереси фірми.

Організаційні гарантії формуються шляхом розробки, побудови й підтримки високої працездатності загальної організаційної структури керування процесом виявлення й придушення погроз діяльності фірми, використання ефективного механізму стимулювання її оптимального функціонування, що відповідає підготовки кадрів.

Матеріальні гарантії формуються за рахунок виділення й використання фінансових, технічних, кадрових, інтелектуальних, інформаційних й інших ресурсів фірми, що забезпечують своєчасне виявлення, ослаблення й придушення погрози, запобігання й локалізацію можливого збитку, і створення сприятливих можливостей й умов діяльності фірми. Дані гарантії наповнюють нормативні й організаційні міри безпеки практичним змістом, створюють реальну основу розвитку культури безпеки фірми.

5.) **Основні заходи** контрольно-пропускного режиму розробляються службою безпеки й затверджуються керівником фірми й оформляються інструкцією про контрольно-пропускний режим. Відповідальність за ор-

ганізацію контольно-пропускного режиму покладає на начальника служби безпеки. Практичне здійснення контольно-пропускного режиму покладає на охорону (чергових по КПП, контролерів, охоронців), працівники якої повинні знати встановлені на об'єкті правила контольно-пропускного режиму, що діють документи один по одному пропуску на об'єкт (з об'єкта) співробітників і відвідувачів, ввозу (вивозу) товарно-матеріальних цінностей. Контольно-пропускний режим може бути встановлений як у цілому по об'єкті, так й в окремих корпусах, будинках, відділах, сховищах й інших спеціальних приміщеннях.

6.) **Вимоги** по контрольно-пропускному режимі повинні бути доведені в обов'язковому порядку до кожного співробітника об'єкта. Всі робітники та службовці об'єкта зобов'язані дотримувати їх. По кожному випадку порушення контольно-пропускного режима повинне проводиться адміністративне розслідування.

Обов'язки охорони по контрольно-пропускному режимі визначається в інструкції й у посадових обов'язках контролерів контрольно-пропускних пунктів.

Підготовка вихідних даних для розробки контрольно-пропускного режиму

Підприємництво і заборона (обмеження) - по своїй природі суперечливе. Мистецтво розроблювача контольно-пропускного режиму полягає саме в тім, щоб знайти розумне сполучення заборони (обмежень) і інтересів підприємницької діяльності фірми.

Розробка заходів і нормативних документів контольно-пропускного режиму починається з визначення вихідних даних. Оцінюючи вихідні дані, розроблювач визначає основні положення інструкції про контрольно-пропускний режим. Доцільно запропонувати наступну послідовність визначення й оцінки вихідних даних.

1. Організаційна структура фірми, місця розташування його окремих елементів і характер виробництва (діяльності) на них. З'ясування цих питань дозволяє вирішити наступні практичні завдання:

- виділити об'єкти, площадки, будинки, приміщення на які необхідно організувати контрольно-пропускний режим;

- визначити характер контрольно-пропускних пунктів (КПП) для пропуску співробітників, транспортних засобів.

2. Провести оцінку "добового обсягу" потоків транспортних засобів, вантажів, матеріальних цінностей і людей (персоналу фірми й відвідувачів) минаючих через КПП й в окремі будинки (приміщення). Тільки на основі оцінки реального стану місць пропуску можна оцінити пропускну здатність діючих КПП і привести її у відповідність із завданнями основного виробництва на об'єкті. Така оцінка дозволить вибрати оптимальний варіант автоматизації й контролю проходу, проїзду на охоронювані території.

3. Виділити на території (по ступені важливості) категорії об'єктів, транспортних засобів і вантажів, а також категорії осіб, що перетинають установлені границі. Для досягнення чіткості у визначеннях пропонується приміщення й територію об'єкта класифікувати залежно від умов доступу й ступеня захищеності на шість категорій режимності ("зон безпеки")

Класифікація категорій режимності наведена в таблиці [1]

Як видно з таблиці, шість категорій режимності здатні охопити практично всі варіанти функціонального призначення службових приміщень. Крім того, таблиця може дати чітку відповідь на питання, які потрібно зробити дії при організації контрольно-пропускного режиму й розробці вихідної документації по встаткуванню об'єкта технічними засобами охорони. Приведення приміщень до однієї з категорій режимності допомагає регламентувати й обґрунтувати:

- умови доступу співробітників підприємства й відвідувачів на об'єкт, визначити загальнодоступного, закритого й обмеженого доступу об'єкти, будинки, приміщення;
- пропозиції адміністрації підприємства по виробленню оптимального варіанта дозвільного порядку пропуску осіб, транспортних засобів і матеріальних цінностей на об'єкт;
- наявність і вид фізичної охорони;
- види використовуваних технічних засобів для забезпечення безпеки.

Таблиця категорій режимності

Категорія зони	Найменування зони	Функціональне призначення	Умови доступу співробітників	Умови доступу відвідувачів	Наявність охорони	Наявність технічних засобів охорони
0	Вільна зона	Місця вільного відвідування	Вільний	Вільний	є	Немає
I	Спостережувана зона	Кімната прийому відвідувачів	Вільний	Вільний	є	Засоби спостереження
II	Реєстраційна зона	Кабінети співробітників	Вільний	Вільний з реєстрацією по документах	Посилена охорона	Охоронна сигналізація
III	Режимна зона	Секретаріат. Комп'ютерні зали. Архіви	По службових посвідченнях	По разових пропусках	Посилена охорона	Охоронна сигналізація, контроль доступу
IV	Зона посиленого захисту	Касові операційні зали. Склади матеріальних цінностей	По спец. пропусках	По спец. пропусках	Посилена охорона	Охоронна сигналізація, система контролю доступу, бар'єри
V	Зона вищого захисту	Кабінети вищих керівників, кімнати для ведення переговорів, сховище	Система контролю дост упу	Система контролю доступу	Посилена охорона	Охоронна сигналізація, технічні засоби інженерне посилення

Розробка інструкцій пропускного режиму

Пропускний режим є невід'ємною частиною загальної системи охорони підприємств. Практичне рішення цих питань оформляється у вигляді "Інструкції про пропускний режим". Зазначена інструкція повинна визначати систему організаційно-правових охоронних мір, що встановлюють дозвільний порядок (режим) проходу (проїзду) на об'єкт (з об'єкта) і може включати:

1. Загальні положення. У цьому розділі вказується:

- нормативні документи, на підставі яких складалася інструкція;

- визначення контрольно-пропускного режиму й ціль його встановлення;
- на кого покладає керівництво пропускним режимом, практичне його здійснення;
- санкції до порушників контрольно-пропускного режиму;
- вимоги до встаткування різних приміщень.

2. Порядок пропуску співробітників підприємства, відряджених осіб і відвідувачів через контрольно-пропускні пункти. У цьому розділі рекомендується:
- перелічити всі КПП й їхнє призначення, опис, розташування й установити їхню єдину нумерацію;
- викласти вимоги до встаткування КПП;
- установити порядок проходу співробітників і відвідувачів на територію об'єкта;
- визначити права й основні обов'язки контролерів КПП;
- установити приміщення, де забороняється приймати відвідувачів і представників сторонніх організацій.

3. Порядок допуску на об'єкт транспортних засобів, вивозу продукції, документів і матеріальних цінностей. У цьому розділі вказується:
- порядок допуску на територію об'єкта (з об'єкта) автотранспорту;
- в'їзд і стоянка на території об'єкта транспорту, що належить співробітникам на правах особистої власності;
- порядок пропуску автомашин сторонніх організацій, що прибули з вантажем на адресу об'єкта в робочий і неробочий час;
- порядок вивозу (ввозу) товарно-матеріальних цінностей;
- правила оформлення документів на вивіз (винос) матеріальних цінностей з території об'єкта.

4. Види пропусків, порядок їхнього оформлення. У цьому розділі визначається:
- види пропусків, їхня кількість і статус;
- опис пропусків;
- порядок оформлення й видачі пропусків;
- загальна заміна й перереєстрація пропусків;
- заходу при втраті пропуску співробітником.

5. Обов'язки посадових осіб по підтримці контрольно-пропускного режиму.

6. Облік і звітність, порядок зберігання пропусків, печаток.

Залежно від структури підприємства й характеру його діяльності інструкція може містити й інші розділи.

Види пропусків

Для допуску на підприємство, в окремі приміщення, як правило, установлюється кілька видів пропусків. Це можуть бути: постійні, тимчасові, разові й матеріальні пропуски. Зразки бланків пропусків розроблятися адміністрацією об'єкта (службою безпеки). По своєму зовнішньому вигляді й змісту пропуски повинні відрізнятися друг від друга й мати захисні властивості. Всі види пропус-ків, за винятком матеріальних, оформляються й видаються бюро пропусків (або іншим підрозділом) за письмовими заявками. Види пропусків визначаються в залежності від специфіки підприємства.

1.) **Постійні пропуски** видаються співробітникам об'єкта, прийнятим на постійну роботу, а так само працівникам інших організацій, закріплених для постійного обслуговування об'єкта. Постійні пропуски можуть ділитися на групи, їхня кількість і призначення визначається інструкцією про контрольно-пропускний режим. Постійні пропуски можуть зберігатися як на руках у співробітників об'єкта, так й у кабінах на КПП. Постійні пропуски осіб, що убувають із об'єкта на тривалий час (відпустка, хвороба, відрядження й т.п.), здаються на зберігання в бюро пропусків (відділ кадрів), а при залишенні таких пропусків у кабіні, на осередку (де зберігається пропуск) робиться відповідна оцінка. Пропуски звільнених з роботи знищуються встановленим порядком.

2.) **Тимчасові пропуски** видаються особам працюючим за контрактом, що перебуває на тимчасовій роботі, прикомандированих до підприємства й зберігаються, як правило, на КПП. Термін дії й порядок

оформлення тимчасових пропусків визначається інструкцією про контрольно-пропускний режим.

Тимчасові пропуски можуть бути з фотографією й без фотографії. Тимчасові пропуски без фотографії дійсні тільки при пред'явленні документа (підтверджуючий особистість.)

3.) **Разові пропуски** (для відвідувачів і клієнтів) видаються на одну особу й тільки для разового відвідування підприємства і його підрозділів. Пропуск оформляється й дійсний при наявності документа особистості. Разові пропуски повинні періодично мінятися по кольорі бланків й інших відмітних ознак. Разовий пропуск виданий водієві транспортного засобу може служити одночасно й разовим пропуском для транспорту. Разовий пропуск дійсний для входу на територію об'єкта або його підрозділу у режимі певного часу. Контроль за відвідуванням підприємства по разовому пропуску здійснюється за допомогою оцінки на зворотному боці пропуску, де вказується час відвідування, завірене підписом особи відвідувача, що прийняв.

Разовий пропуск вилучається на пості контролером, при виході відвідувача з об'єкта й здається в бюро пропусків. Про особу, яка не вийшли з об'єкта по витіканню вказаного терміну дії пропуску, контролер доповідає начальникові варти (черговому по КПП) для вживання заходів по з'ясуванню причин затримки. Прізвища осіб, що відвідали об'єкт по разовому пропуску можуть записуватися в спеціальну книгу обліку.

4.) **Матеріальні пропуски** для вивозу (виносу) товарно-матеріальних цінностей видаються адміністрацією підприємства. Термін дії пропуску визначається інструкцією про контрольно-пропускний режим. Матеріальні пропуски повинні вилучатися на КПП і здаватися в бюро пропусків.

Зразки діючих пропусків повинні перебувати на КПП. Для навчання працівників охорони виділяється необхідна кількість зразків пропусків.

Устаткування контрольно-пропускного пункту

Для організації пропускного режиму на підприємстві обладнаються контрольно-пропускні пункти. Устаткування КПП повинне забезпечувати необхідну пропускну здатність і можливість ретельної перевірки пропусків, документів у минаючих осіб, огляду всіх видів транспорту, перевезення вантажів і задовольняти наступним вимогам:

- виключати можливість несанкціонованого проникнення через КПП на об'єкт (з об'єкта) людей і транспортних засобів;

- сприяти скороченню часу на перевірку документів, огляд транспорту й матеріальних цінностей;
- сприяти виключенню (відомості до мінімуму) помилок охоронця при пропуску людей і транспорту;
- забезпечувати міри безпеки охоронця при огляді транспортних засобів;

Всі види КПП повинні бути обладнані необхідними видами зв'язку й тривожної сигналізації для виклику резерву охорони. На КПП рекомендується розташовувати внутрішній телефон і список телефонів адміністрації підприємства.

КПП для проходу людей

Для контролю осіб минаючих на об'єкт й в окремі будинки (приміщення) будуються КПП. Кожне людське КПП рекомендується обладнати: кімнатою для охорони, кімнатою для огляду громадян, камерою схову, гардеробом, турнікетом з фіксуючими устроями-запорами.

Розміщення приміщень визначаються проектами й залежить від засобів механізації, автоматизації КПП й особливостей підприємства. У контрольно-пропускному залі влаштовуються проходи, які обладнаються технічними засобами охорони й фізичних бар'єрів. У комплект устаткування, як правило, входить:

- засобу механізації, автоматизації, системи контролю доступу;
- фізичні бар'єри (огородження турнікети, хвіртки;
- основне й резервне висвітлення;
- засобу зв'язку й тривожної сигналізації;
- системи відеоконтролю.

Як засоби контролю доступу можуть використатися різні турнікети. Турнікети призначені для керування потоками людей і регулювання входу (виходу). Останнім часом найбільш широке поширення одержали электромеханічні турнікети. Ці турнікети, у відмінності від громіздких і незручних у керуванні механічних, легко управляються з пульта охоронця й можуть працювати в складі автоматизованої системи контролю доступу.

При виборі турнікета потрібно знати, як вони бувають "нормально відкриті" й "нормально закриті". "Нормально відкриті" турнікети (наприклад, розсувні, які донедавна були встановлені в російському метро) у світовій практиці використаються досить рідко. Вони можуть ударити минаючу людину й не дозволяють здійснювати ефективний контроль.

Для здійснення надійного контролю частіше використаються “нормально закриті” турнікети: роторні турнікети-"вертушки", турнікети-триподи й хвіртки.

1.) **Хвіртки** застосовуються для керування потоками людей - організації - організації вільного проходу в одну сторону (на вхід або вихід) і заборони проходу в іншу. Хвіртки широко використаються в магазинах, аеропортах, вокзалах. Застосування хвірток для контролю доступу неефективно, це пов’язане з тим, що хвіртки не розділяють потік людей по одному, тому що після відкриття хвіртки через неї можуть пройти кілька людей. Хвіртки можуть установлюватися для організації вільного виходу, у той час як контроль входу довіряють триподам або “вертушкам”.

2.) **Турнікети-триподи** із трьома планками, що перепиняють, є одним їх найбільш оптимальних засобів для здійснення контролю санкціонованого проходу. Триподи мають сучасний елегантний вид і легко монтуються. Триподи дозволяють здійснювати ефективний контроль доступу, тому що розділяють потік людей по одному, забезпечуючи при цьому високу пропускну здатність. Триподи можуть застосовуватися в системах електронних прохідних, у тому числі в умовах великого потоку людей. Для запобігання можливості підлізти під планки турнікета або перестрибнути через них, на турніку рекомендується встановлювати спеціальні датчики, які спрацьовують при спробі несанкціонованого проходу.

3.) **Роторні турнікети** - "вертушки" застосовуються в тих випадках, коли необхідно повне перекриття зони проходу. Вони можуть бути різними по висоті - від поясних до турнікетів у повний ріст, які конструктивно подібні до обертових дверей.

Автотранспортні КПП

До складу автотранспортного КПП входить оглядові площадка й службові приміщення.

1.) **Оглядова площадка** призначається для огляду автомобілів при їхньому виїзді. Оглядові площадки можуть розташовуватися, як на території підприємства, так і за її межами, на місцевості, безпосередньо пов’язаною з основними воротами КПП.

Оглядова площадка повинна відповідати наступним вимогам:

- мати достатню площу для розміщення транспорту, що оглядається, технічні засоби для забезпечення нормальних умов роботи охоронця;

- виключати можливість несанкціонованого проникнення на об'єкт (з об'єкта) людей і транспортних засобів;
- забезпечувати при встановленій інтенсивності руху, у будь-який час доби й року, огляд автомобільного транспорту й перевезених вантажів;
- бути ізольованої від інших споруджень, що не має відносини до охорони об'єкта й устаткуванню КПП;
- забезпечувати міри безпеки охоронця при виконанні своїх обов'язків.

Розміри оглядової площадки встановлюються залежно від габаритів транспорту й перевезених вантажів. Більш детально на цю тему ми поговоримо на семінарських заняттях

Автотранспортні КПП можуть обладнатися світлофорами, вагами для зважування автомобілів, оглядовою ямою або естакадою для огляду вантажів, механізованими пристроями для автоматичного відкриття й закриття воріт з фіксаторами.

Оглядові площадки по периметрі обладнаються фізичними бар'єрами й рубежем сигналізації. Площадки, як правило, вигороджуються забором з металевої сітки або декоративних ґрат висотою до 2,5 метрів. На площадці обладнаються основні й допоміжні механізовані ворота. Основні ворота встановлюються на лінії основного огородження об'єкта, а допоміжні на протилежній стороні оглядової площадки. Замість воріт можуть застосовуватися механізовані шлагбауми. На автомобільних КПП використаються ворота з обмеженням і без обмеження габаритів по висоті. По конструкції вони можуть бути розстібними або розсувними (висувними). Розстібні ворота повинні обладнатися фіксаторами.

Для регулювання руху транспорту, що проходить через проїзди оглядових площадок КПП можуть застосовуватися двосекційні світлофори з лінзами червоний і зелений кольори.

До складу електромеханічного встаткування КПП для автомобільного транспорту звичайно включаються:

- ✸ електродвигуни, привід воріт;
- ✸ кінцеві вимикачі, автоматичного відключення електродвигунів при повністю закритих і відкритих стулках воріт;
- ✸ магнітні пускачі електродвигунів;
- ✸ електроустаткування світлофорів;
- ✸ кабельні, силові лінії.

Груповий розподільний щит (щит керування) може встановлюватися в приміщенні КПП, а при відсутності будинку КПП у спеціальній металевій шафі безпосередньо на оглядовій площадці.

Пропуск співробітників та відвідувачів на об'єкт

Прохід співробітників і відвідувачів на територію об'єкта, у спеціальні підрозділи й назад здійснюється по встановленим на об'єкті пропускам, через контрольно-пропускні пункти. Пропуск повинен бути основним документом, що дає право на прохід.

Допуск відряджених (відвідувачів) виробляється по тимчасовим. Разовим пропускам у встановлені й зазначені в пропуску годинники, у виняткових випадках по затвердженим начальником служби безпеки спискам із пред'явленням документів, що засвідчують особистість.

Представники засобів масової інформації допускаються на об'єкт на загальних підставах у супроводі представників адміністрації.

У неробочий час, вихідні й святкові дні допуск співробітників на об'єкт повинен бути обмежений і вироблятися за попередніми заявками (спискам) керівників підрозділів, завізованими начальником служби безпеки, із пред'явленням постійного пропуску. На підприємствах зі змінним режимом роботи до пропуску можуть видаватися спеціальні вкладиші змінності.

Чергові спеціальних служб об'єкта (електрики, сантехники, працівники зв'язку й т.д.), що працюють позмінно, допускаються на територію об'єкта в неробочий час, у вихідні й святкові дні по списках, підписаним начальниками відповідних служб і затвердженими начальником служби безпеки.

На підставі чинного законодавства й рішення адміністрації окремі категорії осіб користуються правом проходу на об'єкт без пропуску, при пред'явленні службового посвідчення, це:

- працівники прокуратури;
- працівники міліції по територіальності своєї роботи;
- інспектори праці, котлонадзору, енергонагляду по територіальності своєї роботи;
- посадові особи й окремі категорії працівників санітарно-епідемічної служби органів охорони здоров'я, що здійснюють санітарний нагляд.

Категорії осіб що мають право проходу на об'єкт без пропуску (по службових посвідченнях) повинні бути чітко вказані в інструкції про контрольно-пропускний режим.

З метою здійснення пропускного режиму на території об'єкта й у його структурних підрозділах наказом начальника підприємства затверджується перелік категорійних підрозділів (приміщень), сховищ. У цих приміщеннях установлюється спеціальний режим і підвищена відповідальність за його дотримання працівниками цих підрозділів.

Допуск у ці приміщення здійснюється строго за списком, погодженому зі службою безпеки. Прийом відвідувачів сторонніх організацій і підприємств, як правило, максимально обмежується.

У всіх приміщеннях категорійних підрозділів повинні бути вивішені в засклених рамках списки працівників, що мають допуск у ці приміщення. Всі приміщення по закінченні робіт оглядаються черговими по підрозділах й особами, відповідальними за їхній протипожежний стан. Електрика й електронагрівальна апаратура знеструмлюється, вікна й кватирки закриваються, двері защіпаються на замок й опечатуються. По закінченні робочого дня обладнані охоронною сигналізацією категорійні приміщення, спецсховища, склади й ін. об'єкти закриваються й опечатуються відповідальними особами цих підрозділів. Приміщення здаються під охорону варти. Представник охорони перевіряє сигналізацію в присутності працівників, що здають приміщення. Ключі від цих приміщень в опечатаних пінах здаються під розписку начальникові варти.

Одержання ключів, розкриття приміщень, обладнаних охоронною сигналізацією, роблять люди, що мають допуск на право розкриття цих приміщень із пред'явленням постійного пропуску. Списки осіб, що мають право розкривати (закривати) зазначені приміщення із вказівкою номерів печаток, який опечатуються приміщення й номерів службових телефонів, підписуються начальником підрозділу й затверджуються начальником служби безпеки.

Всі особи, що намагаються пройти через КПП без пред'явлення пропуску або по чужому, неправильно оформленому пропуску, пронести на об'єкт (з об'єкта) заборонені предмети, затриму-ються й передаються в службу безпеки підприємства. По кожному факті затримки начальник варти або черговий по об'єкті становить службову записку про порушення пропускного режиму.

Допуск на територію підприємства транспортних засобів, вивіз матеріальних цінностей

Допуск на територію (з території) підприємства транспортних засобів, що належать підприємству, дозволяється при пред'явленні водієм особистого пропуску зі спеціальним шифром або транспортним пропуском і шляховим аркушем. Вантажники й супровідні особи, що випливають із транспортом, пропускаються через КПП на загальних підставах.

Всі транспортні засоби при проїзді через КПП піддаються огляду. В'їзд і стоянка на території підприємства транспорту, приналежним співробітникам на правах особистої власності дозволяється по спеціальних списках.

Автомашини сторонніх організацій, що прибули з вантажем на адресу підприємства в робочий час, допускаються на територію по службових записках з оглядом на автотранспортному КПП.

В'їзд машин на територію підприємства дозволяється штатним водієм у супроводі представника адміністрації (вантажоодержувача).

Залізничний транспорт й обслуговуючі його бригади пропускаються на підприємство по пропусках установленого зразка, по списках або іншому порядку встановленим інструкцією про пропускний режим. Для пропуску й огляду залізно-дорожнього транспорту від підрозділу охорони виділяється оглядова група.

Опломбовані вагони й контейнери, пропускаються через КПП послу їхнього зовнішнього огляду, якщо відбитки пломб відповідають відбиткам у супровідних документах або накладних. У випадку невідповідності відбитків, виявлення проламів вагона (контейнера) або обриву пломби вагон (контейнер) підлягає розкриттю й огляду в присутності представників адміністрації й залізниці .

Вивіз і винос готової продукції й інших матеріальних цінностей з території об'єкта здійснюється по матеріальних пропусках установленого зразка.

Переконавшись у правильності оформлення документів й їхній повній відповідності з указаними цінностями, охоронець залишає на КПП пропуск, ставить на пропуску дату й час вивозу вантажу, розписується й дає дозвіл на вивіз матеріальних цінностей.

Всі документи що вивозять (що виносять) з підприємства матеріальні цінності реєструються в бюро пропусків по книзі обліку й плині наступного дня передаються в бухгалтерію. Бланки всіх видів матеріальних пропусків виготовляються типографським способом і зберігаються в

бухгалтерії, видаються в підрозділи підприємства по службових записках. Документи на вивіз (винос) матеріальних цінностей повинні бути виписані тільки на та кількість вантажу (місць, ваги й т.п.), що може бути вивезене (винесено) одночасно й дійсні тільки на дату, зазначену в дозвільному документі.

Будівельні й деревні відходи, макулатуру, металобрухт, металеву стружку рекомендується вивозити з території підприємства по накладній, як матеріальні цінності. Вивіз із території об'єкта різного сміття, землі й снігу може вироблятися без оформлення документів, але з обов'язковою реєстрацією на автотранспортному КПП.

Контроль за транспортними засобами, що в'їзджають (виїзджають) з\на підприємство, рекомендується проводити в наступній послідовності.

Працівник охорони, переконавшись у правильності оформлення супровідних документів повинен упевнитися у відповідності найменування й кількості ввезеного (або що вивозять) вантажу з даними, що вказані у супровідних документах, а також перевірити сховані місця транспортного засобу (які можуть використатися для розкрадання). Із цією метою він оглядає транспортний засіб і вантаж, використовуючи спеціальну оглядову площадку, естакаду. Матеріальні цінності на транспортному засобі повинні бути покладені в певному порядку, зручному для контролю. При пропуску опломбованих (опечатаних) вантажів охоронець звіряє пломби (печатки) із зазначеними в накладних, після чого, коли ні яких сумнівів у відповідності кількості й найменування вантажу супровідним документам ні, дозволяється в'їзд або виїзд автотранспорту. Матеріальні пропуски, товаротранспортні накладні реєструються охоронцем у книзі обліку (окремо на ввезені й вивезені грузи,) у строгій відповідності з порядком їхнього надходження.

Критерії ефективності роботи охоронного підрозділу

Основними критеріями ефективності роботи охоронного підрозділу є ступінь захищеності від несанкціонованого проникнення на охоронюваний об'єкт і ступінь забезпечення фізичної безпеки охоронюваних осіб. Показниками першого критерію (ступінь захищеності від несанкціонованого доступу на охоронюваний об'єкт) є:

1) - сума викраденого майна з вини охоронного підрозділу;

2) - кількість припинених спроб фізичних осіб проникнути на охоронюваний об'єкт;

3) - кількість випадків затримки співробітників підприємства за винос викраденого майна;

4) - кількість осіб, затриманих і притягнутих до кримінальної відповідальності за здійснення проти охоронюваного об'єкта майнових злочинів;

5) - кількість осіб, затриманих і притягнутих до адміністративної відповідальності за здійснення майнових правопорушень.

Інший критерій (ступінь забезпечення фізичної безпеки охоронюваних осіб) розкривається за допомогою наступних показників:

1) - кількість відвернених замахів на життя й здоров'я охоронюваної особи;

2) - кількість припинених насильницьких злочинів проти охоронюваної особи;

3) - кількість осіб, затриманих при спробі проникнення на охоронюваний об'єкт із метою здійснення насильницьких злочинів проти спеціально не охоронюваних співробітників персоналу;

4) - кількість реалізованих злочинцями замахів на охоронювану особу.

7.3. Забезпечення безпеки посадових і офіційних осіб

Все більша кількість відомих і багатих людей і членів їхніх родин стають об'єктом погроз із боку терористів, викрадачів, незадоволених співробітників і божевільних. У результаті цього як ніколи раніше зріс попит на фахівців, які можуть забезпечити захист посадових й офіційних осіб. Як відзначив Э. Дж. Крискуоли, виконавчий віце-президент Американського Суспільства Промислової Безпеки (ASI): "Раніше в нас ніколи не було проблем по забезпеченню безпеки посадових й офіційних осіб".

Коли Э. Дж. Крискуоли почав у середині 50- х років свою діяльність в області забезпечення безпеки, "єдиною людиною, що перебував під захистом, був президент США. У цей час існують деякі корпорації, у яких питання забезпечення безпеки виконавчих директорів відповідають рівню захисту президента Сполучених Штатів". "Це чисто питання економіки", - говорить Э. Дж. Крискуоли. Якщо що-небудь трапиться з директором, це

може привести до негативних наслідків для всієї компанії й може несприятливо відбитися на її акціях. Він уважає, що забезпечення безпеки посадових й офіційних осіб є чимсь начебто страхової політики.

Для із проблем, пов'язаних з більшою кількістю погроз, сьогодні потрібно дещо більше, ніж мати, як сказав один спостерігач, "здоровенних хлопців з маленькими голівками й більшими куркулями в кишенях". Тут потрібні кваліфіковані добре навчені професіонали. Нижче з деякі рекомендації з вибору, обігу й повсякденній роботі з вашими охоронцями, а також по оцінці їхніх здатностей.

Вибір охоронця

Не вибирайте «Брудного Гари» в охоронці. Робота має мету, виключення погрози, тому охоронців необхідно підбирати по розмірі їхніх мозків, а не по ширині їх плечей. За всяку ціну уникайте охоронців, які вважають, що основним їхнім призначенням є ведення перестрілки із супротивником.

У цей час росте число жінок-охоронців, тому що в них більше розвинені професійні якості в цій області й вони справляються зі своїми обов'язками дуже добре. Ви виявитеся в лиху, якщо ваш охоронець сподівається головним чином на свою вогнепальну зброю й свої мускули, а не на професійні навички й досвід. Надійне забезпечення безпеки має на увазі насамперед розумові здатності, уміння міркувати здраво й натреніровано. Як правило, навіть багато охоронців навряд чи врятують ваше життя, якщо ви потрапите в пастку з вини своєї служби безпеки.

Коли Альдо Моро, лідер італійських християн-демократів, був викрадений насильницьким шляхом, охоронці, що супроводжували його, були вбиті терористами. Тільки один охоронець зміг вибратися з автомобіля й відкрити відповідний вогонь, однак і він був застрелений снайпером, що перебував на даху.

Аналогічний випадок відбувся з німецьким промисловцем Гансом Мартіном Шляєром, що в першу чергу охоронці, які супроводжували його в другій машині були вбиті, ніж вони зуміли відкрили відповідний вогонь. Запитаєте будь-якого ветерана війни й він відповість вам, що засідки звичайно бувають кривавим швидкоплинним заходом, де ініціативою володіє тільки нападаюча сторона. У такий спосіб вам потрібні охоронці, які б відповідали за те, щоб ви не потрапили в лихо, і змогли б у випадку небезпеки професійно виконати свої обов'язки.

Більше - не завжди означає краще. Деякі посадові особи наполягають на тому, щоб їх оточували ціла юрба амбалів з товстими шиями, які могли заслонити їх від куль. Покладайтеся на декількох надійних людей, які можуть ворушити своїми мозками й мають здоровий глузд.

Непомітність

Кращими охоронцями є люди непомітні й непримітні, хоча в деяких випадках буває необхідна демонстрація сили, як стримуючого фактора. Якщо у вас тільки один або два охоронці, вони не повинні перебувати пліч-о-пліч із вами для того, щоб нападаючий не зміг визначити, хто вони такі. У цьому випадку нападаюча сторона спочатку вб'є їх, а потім прийметься за вас.

Досвід

Ваші охоронці повинні бути кваліфікованими й досвідченими фахівцями. Не робіть охоронцем нікого, просто віддавши йому зброя, як це робиться в деяких країнах третього миру. Як правило, кращими охоронцями є колишні секретні агенти, що були військовослужбовцями підрозділу Дельта, Альфа, ФСБ, СБУ й ФБР, а також офіцери правоохоронних органів з досвідом роботи в області забезпечення безпеки. Крім цього, на деяких приватних курсах готовлять компетентних і здатних охоронців. Тому остерігайтеся випускників так званих шкіл " Бистро "за кілька діб і курсант з поганою вивченою програмою навчання – отримує «диплом» охоронця.

Помніть, що Служба безпеки - це дуже велика організація, у якій працюють співробітники, що виконують виконувати різну роботу. Але не кожен співробітник Служби безпеки має відповідні навички й досвід. Багато посадових осіб компаній уважають, що будь-який співробітник ФСБ, ФБР або СБУ має достатню кваліфікацію для того, щоб бути охоронцем. Багато агентів цих підрозділів займаються тільки тим, що вистежують і заарештовують злочинців, а співробітники СБУ збором й аналізом розвідувальної інформації. Тому, тільки деякі у своїх організаціях є фахівцями з питань забезпечення безпеки й охорони.

Досвід міліцейської, поліцейської і правоохоронної діяльності не обов'язково означає, що людина може стати охоронцем. Багато колишніх працівників МВС, СБУ та ФСБ стали гарними охоронцями, однак додаткова підготовка не стане зайвої і для них.

Не бійтеся знайти способи, щоб ретельно вивчити досьє своїх потенційних охоронців. Помніть, що більшість фахівців навіть співробітни-

ки Секретної Служби ніколи не були в дійсно небезпечній ситуації й не зустрічалися з реальною погрозою віч-на-віч . Якщо вам загрожує небезпека, вам потрібні охоронці, які вже побували в таких колотнечах. Остерігайтеся шахраїв, хвальків і тих, хто думає і удає із себе фахівців.

Не вірте розповідям тих, хто розповідає про свої геройські подвиги, щоб зробити на вас сприятливе враження. По можливості перевірте послужний список, рівень професіоналізму, а також наявність нагород і бойових медалей можливих претендентів. Не довіряйте тим, хто говорить, що його досьє є секретним; навіть тих людей, які раніше займали ключові урядові пости, ми завжди можемо перевірити їхній послужний список і колишній рід їхньої діяльності.

Ініціативні й думаючі охоронці

При відборі охоронців сконцентруйтеся на тих, які можуть передбачати проблеми з мінімальною часткою наставництва й підказок. Ви не можете думати за вашого охоронця. Найчастіше ви будете зайняті іншими справами, і тому ваші охоронці будуть єдиними людьми, які цілодобово повинні займатися питаннями безпеки. На перший план ставимо: контактність, передбачливість, відповідальність і розсудливість. Куди б ви не пішли, ваш охоронець заздалегідь повинен передбачити й продумати всі заходи щодо забезпечення вашої безпеки. Тому він повинен мати здатність налагоджувати усні контакти й вести письмову переписку. Він буде вашим представником, а тому його поводження буде відбиватися на вас і вашої компанії. Наполягайте на відповідальності, розсудливості й професіоналізмі.

Посада охоронця Дуже Важливої Особи може закрутити голову. Вам не потрібний охоронець, що буде прокладати вам шлях, використовуючи свою нахабність і пробивні здатності. Його зарозумілість створить несприятливе враження про вас. Підбирайте охоронців, які можуть працювати тихо й ефективно, не створюючи ажіотажу. Підшукуйте холоднокровного охоронця. Нервовий і неврівноважений охоронець зведе вас із розуму.

Утворення, зовнішній вигляд, знання іноземних мов

Утворення є дуже важливим фактором у роботі охоронця, тому що це допоможе йому зрозуміти, чим ви займаєтеся. У цьому зв'язку у вашого охоронця не виникне проблем під час прийомів, відвідування дорогих ресторанів і проживання в респектабельних готелях. Деякі програми забезпечення безпеки включають курси навчання гарним манерам, підбора одягу,

вибору маршрутів подорожей і поводження за столом. Вашим охоронцям варто одягатися так само як і ви (тобто відповідно ситуації). Якщо ви запрошені на обід, під час якого на вас повинен бути чорна краватка, ваш охоронець також повинен мати чорну краватку. Яскрава краватка не підходить до темному добре зшитому діловому костюму. Якщо ви часто виїжджаєте за кордон, було б добре, якщо один або кілька охоронців розмовляли мовою країни перебування. Гарне знання іноземної мови буде корисно не тільки для організації звичайної роботи, налагодження й підтримки ділових контактів, але й надасть неоціненну допомогу у важкій ситуації, при дозволі конфліктів і дозволить адекватно реагувати на погрози.

Самодисципліна. Звертайте особливу увагу на самодисципліну своїх охоронців. Робота охоронця часом буває нудна, і охоронці можуть розслабитися. Терорист чекає саме того моменту, коли ваш охоронець відлучиться для того, щоб подзвонити по особистих справах або випити склянка води.

Фізичний стан. Ваші охоронці не повинні виглядати горою м'язів, однак гарний фізичний стан є важливим чинником, особливо якщо ви захоплюєтеся щоденними пробіжками. Вам не потрібні охоронці, які не можуть поспіти за вами. У теж самий час вони повинні встигати за вами й у повсякденних справах, особливо якщо ви багато працюєте й подорожуєте. Ваші охоронці часто будуть залишатися чергувати, коли ви вже заснете, і повинні будуть вставати ще до вас. Охоронець, що не має гарної фізичної форми, не зможе адекватно відреагувати на надзвичайну ситуацію. Цілодобове забезпечення безпеки. Помнете, що для того щоб забезпечити цілодобовий захист, необхідно організувати чергування служби охорони в три зміни по 8 годин. Якщо ви вирішите зробити зміни дві по 12 годин, ваші охоронці будуть мати дуже більше навантаження, що приведе до зниження ефективності їхньої роботи. Однак трьохзмінне чергування є дорогим задоволенням, тому зважте все за й проти.

Медична підготовка. Ваші охоронці повинні бути навчені правилам надання першої медичної допомоги й реанімації за допомогою штучного дихання й закритого масажу серця. Вони повинні бути здатні швидко й правильно надати медичну допомогу й знать куди й кому подзвонити для виклику додаткової допомоги. Постачите ваших охоронців всією необхідною інформацією про вас і членах вашої родини, включаючи історію хвороби, перелік ліків і медикаментів, які ви звичайно приймаєте,

алергійні реакції, щеплення, приписання лікаря на контактні лінзи для корекції зору, а також імена, спеціальності й телефонні номери ваших домашніх лікарів.

Пістолети й інша зброя. Охоронці повинні мати професійні навички володіння зброєю й уміти застосовувати його в бою. Однак остерігайтеся охоронців, які приділяють занадто багато уваги вогнепальній зброї. Якщо вам повезе і якщо ваш охоронець буде виконувати свою роботу належним чином, вам ніколи не знадобиться вогнепальна зброя. Таким чином, уміння вашого охоронця звертатися зі зброєю не цінується занадто високо в порівнянні з іншими його достоїнствами.

Ігноруйте такі рекламні оголошення, як: "Колишній агент шукає одноразову роботу. Маю навички обігу з холодною зброєю, автоматичною вогнепальною зброєю, а також з вибуховими пристроями". Якщо ваші охоронці носять зброю, переконайтеся, що вони вміють користуватися нею. Нервовий і неврівноважений збройний охоронець є міною вповільненої дії - він може заподіяти шкоду вам і стороннім людям. Охоронці повинні виймати зброю тільки якщо буде потреба. Варто регулярно приймати від них заліки по володінню вогнепальною зброєю, Визначите строгі правила випадків застосування зброї, наприклад, зброя повинне застосовуватися тільки у випадку наявності загрози життю і як остання міра для усунення цієї погрози.

Ваші охоронці повинні справлятися з усіма погрозами й надзвичайними ситуаціями без застосування вогнепальної зброї. Остерігайтеся "ковбоїв", озброєних зброєю, що не пристосована для забезпечення захисту, наприклад, Магнум .44, куля якого може пробити кілька стін і випадково вбити або ранити вас або членів вашої родини. Якщо ваші охоронці ззброєні, переконайтеся, що носіння ними зброї відповідає загальним і місцевим законам і правилам. Розглянете також можливість придбання поліса страхування на випадок загибелі або поранення вашого охоронця або на випадок, якщо в результаті застосування вогнепальної зброї вашим охоронцем постраждає стороння людина.

Школи навчання заходам щодо забезпечення безпеки

Ознайомтеся із програмами навчання, надаваними різними школами безпеки. У той час як деякі з них мають солідну репутацію й випускають добре підготовлених і кваліфікованих фахівців, інші не відповідають своєму призначенню. Для того, щоб мати обґрунтоване судження, поцікавтеся досвідом інструкторів, розподілом колишніх випускників, а

також назвами компаній й організацій, які направили своїх співробітників для навчання в цих закладах. Майте на увазі, що одне-двотижневі курси не зроблять кваліфікованим фахівцем шофера або охоронця. Краще не мати ніякої підготовки, чим мати короткострокову підготовку, тому що при цьому в людини створюється помилкове почуття прилучення до питань безпеки й здатності виконувати свої обов'язки.

Робота з охоронцями

Основним правилом роботи з охоронцями - це завжди слухати, що охоронці хочуть вам сказати. Охоронці є вашими особистими консультантами з питань безпеки, яким доручено передбачати ваші щоденні вимоги в цій області. Як посадова особа ви, безсумнівно, знаєте як керувати, як приймати рішення, коли й куди піти без необхідності консультуватися з ким би те не було. Завданням охоронця з погляду забезпечення безпеки є постачати вас радами й рекомендаціями в тім, що стосується вашої повсякденної діяльності. Якщо ви не прислухаєтеся до думки своїх охоронців, навіщо мати саму охорону?

Вимоги по забезпеченню безпеки найчастіше мають вузьку спрямованість і необхідний час для їхнього перетворення в життя. Один з колишніх охоронців президента Кеннеді говорив, що президент мав звичай по ночах ходити по Овальному кабінеті в Білому домі "як звір у клітці", тому що він не міг піти куди-небудь, не залучаючи до себе підвищеної уваги. Очікуйте проблем, які можуть виникнути принаймні на первісному етапі формування вашої програми по забезпеченню безпеки. Згодом ваші обережності в цьому зв'язку відійдуть на другий план і стануть складовою частиною вашого способу життя й повсякденних потреб.

Неможливо буди на одинці з самим собою

Наявність охоронців накладає деякий відбиток на особисте життя. Ви не завжди зможете побути один. Більше того, якщо команда ваших охоронців добре виконує свої обов'язки, вони можуть задати вам багато питань, що стосується вашої особистої життя. Якщо ви не скажете своїм охоронцям, що у вас є коханка або що ви є членом який-небудь секс клубу, ви можете порушити їхні плани й наразити на небезпеку вашу особисту безпеку. Помніть, що чим менше слабких сторін ви маєте, тим краще буде ваша безпека.

Якщо викрадачі або терористи спостерігають за вами й виявлять, що ви не берете охоронців у готель, де у вас призначена зустріч із вашою коханкою, вони виберуть саме цей момент для нападу на вас. Забезпечен-

ня захисту типу “пліч-о-пліч ”, що можна часто бачити в кіно, не завжди буває адекватним у багатьох випадках. Якщо ваш охоронець наполягає на тому, щоб завжди перебувати з вами, у нього є підстави на це, і ви повинні врахувати його раду. Він навіть може супроводжувати вас у туалет.

Аналіз погрози

Багато часу буде витрачатися вашими охоронцями на пошук й аналіз ступеня небезпеки, що загрожує вам, для того, щоб знайти найкращий спосіб вашого захисту. Всі погрози у вашу адресу й адресу вашої родини повинні сприйматися серйозно й ретельно аналізуватися. Якщо вам і членам вашої родини загрожують терористи, необхідно збирати інформацію про те, кому конкретно вони загрожують, а також про причини цих погроз, методах можливого нападу, видах зброї й колишніх операцій подібного характеру. У такий спосіб можна повністю оцінити небезпека, що грозить вам і членам вашої родини, і ухвалити рішення щодо забезпечення вашої безпеки.

Перспективне планування. 90% роботи із забезпечення безпеки посадових й офіційних осіб полягає в перспективному плануванні. Ваші охоронці не тільки будуть збирати й аналізувати розвідувальні дані, але вони також будуть заздалегідь намічати маршрути вашого пересування й вести іншу логічну підготовчу роботу, наприклад, узяття напрокат підходящого автомобіля й пошук найближчих медичних установ. Всі ці дії й заходи мають важливе значення для забезпечення вашої безпеки й без них інша ваша програма безпеки буде марною. Ви можете надати допомогу вашим охоронцям у цьому питанні, не жадаючи від них уміння й необхідності читати ваші думки.

Як уникнути небезпеки

Основним завданням охоронця є відгородити вас від небезпеки, і у випадку появи такий він повинен ужити всіх заходів для того, щоб повести вас якнайшвидше з небезпечного місця. У випадку нападу охоронець повинен устати між вами й атакуючими, а потім швидко повести вас. Нейтралізацією нападаючих можна зайнятися після цього. Якщо хто-небудь відкриє по вас вогонь, ваш охоронець повинен кинути вас на землю або вштовхнути в найближче вкриття й закрити вас своїм тілом. Тільки переконавшись, що ви перебуваєте в укритті, охоронець може відкрити відповідний вогонь.

Не потрібно соромитись, якщо вам доведеться рятуватися втечею. Ваші супротивники можуть бути краще збройні й мати перевагу фактора

раптовості. Вашою метою буде залишити небезпечне місце якнайшвидше .Наведемо приклад, якби в єгипетського президента Анвара Садата були більше досвідчені охоронці, вони могли б урятувати його життя. Спочатку вони виявилися ізольованими від нього офіційними особами, що бажають сфотографуватися поруч із президентом. Коли почалася стрілянина, охоронці сховалися й відкрили відповідний вогонь замість того, щоб захищати Садата. Єдиним укриттям їхнього лідера стали стільці, які були кинуті на нього. Агенти американської Секретної Служби, які вважаються найбільш підготовленими фахівцями в цій області, мають звичай відкривати відповідний вогонь із різних позицій, ні чого не змогли вдіяти.

Ваші охоронці повинні контролювати себе, якщо вас обсипають критичними зауваженнями або ображають словесно. Вони не повинні губити розуму й застрахувати вас від неприємностей, а також виявити силу волі, щоб не вдарити образившу вас - людину. Помніть, що необгрунтована брутальність із боку вашого охоронця може стати результатом залучення вас до відповідальності.

Надання допомоги після нападу

Ваш охоронець повинен знати, де перебуває найближча лікарня, а також самий короткий маршрут до її у випадку, якщо ви або член вашої родини одержить поранення. Візьмемо приклад, після того, як президент Рейган був поранений потенційним убивцею, він був негайно відправлений у найближчу лікарню. У той час він тільки відчув біль у грудях, але думав, що одержав просто місцеві забої. Якби агенти Секретної Служби виявили нерішучість, Рейган не зміг би вижити.

Ви повинні виробити план на випадок надзвичайної ситуації. У ньому необхідно вказати з ким необхідно контактувати, хто є старшим, хто повинен спілкуватися із представниками засобів масової інформації, передбачити заходи щодо запобігання нападу на інших членів вашої родини, розташування ваших охоронців у лікарні й т.д. Необхідно відзначити, що коли стріляли в Рейгана, він був на час відділений від свого спеціального, військового помічника, що завжди носить валізку із секретними кодами для запуску ядерних ракет. Помічникові довелося самому добиратися до госпіталю університету імені Вашингтона, де був президент, однак агенти Секретної Служби не дозволили йому ввійти, тому що вони не знали цього помічника і його обов'язків. Поки він сам не знайшов людину, що його знає і засвідчив його повноваження, помічник зміг тільки після цього

приєднатися до президента. Зразу був зроблений аналіз цієї події, були вжиті заходи по недопущенню таких випадків надалі.

Проведення оцінки ваших охоронців

Спостерігайте за вашими охоронцями й зауважуйте, як вони реагують на голосні звуки й різкі рухи. Якщо охоронець дивиться в напрямку джерела збурювання, він має потребу в додатковій підготовці. Першою дією вашого охоронця повинне бути знайти вкриття для вас, а не видивлятися на джерело з. Якщо він бачить небезпеку й намагається оцінити її ступінь, вас у цей час можуть убити. Він повинен бути запрограмований на прояв негайної реакції без усяких роздумів. Гарні програми підготовки охоронців передбачають показ відеофільмів, на яких зняті слухачі курсів у різних ситуаціях, як вони виглядають й як вони реагують на шум і потенційну погрозу. Ви можете поцікавитися, чи проходили ваші охоронці подібну підготовку. Крім цього, ви повинні бути впевнені, що ваші охоронці не відволікаються по дрібницях.

На поданнях, спортивних змаганнях й інших публічних заходах, якщо вас супроводжує один охоронець, він повинен спостерігати за тим, щоб до вас ніхто не дібрався непомітно. Якщо вас супроводжують трохи охоронців, кожному необхідно виділити окремий сектор спостереження, від якого він не повинен відволікатися. Часто важливі особи супроводжуються охоронцями, які відчуваючи побожний страх перед його або її присутністю, дивляться тільки на них, а не юрбу.

Повага. Не звертайтеся з охоронцями, як із хлопчиками 'прийми-подай', або носіями.

Якщо ви очікуєте від них професіоналізму, поважайте їх. Ніколи не просите їх виконувати які-небудь незаконні дії, як наприклад покупка для вас наркотиків, або доставка повії. Звертайтеся з ними так, начебто в один день від них буде залежати ваше життя.

Стеження. Ваші охоронці повинні постійно й уважно стежити за можливим стеженням або спостереженням. Якщо ви йдете пішки, один з ваших охоронців повинен час від часу відходити назад для того, щоб переконатися, що за вами немає стеження. При відсутності небезпеки ваші охоронці повинні використати засоби радіозв'язку для перегляду інших частот і виявлення можливих розмов про вас або яких-небудь підозрілі переговори. Теж саме необхідно проробити й з діапазоном персонального й службового радіозв'язку, якщо така є.

Зв'язок. Ваші охоронці повинні постійно підтримувати зв'язок з командним пунктом або штабом служби безпеки вашої компанії. Коли ви подорожуєте й не перебуваєте в заздалегідь підготовленому місці, ваш охоронець повинен завжди підтримувати зв'язок з вашим командним пунктом/офісом або з місцевою поліцією. Стандартне встаткування включає, (портативні дуплексні радіостанції), а також пристрій звукової сигналізації або пейджер для виклику підмоги або доповіді про ту або іншу проблему. На телефонних апаратах можна встановити пристрій засекречування (скремблери) для ведення секретних переговорів з командним центром або з ким-небудь, що має аналогічне встаткування.

Етикет. У справі забезпечення безпеки з манери не грають великої ролі при визначенні хто за ким повинен пройти у двері. Ваш охоронець повинен проходити першим, щоб розвідати обстановку.

Поїздка на автомобілі. Напад на автомобіль як правило здійснюється з боку водія, тому що нападаючий хоче насамперед зупинити автомобіль. Тому ваш охоронець повинен мати на увазі насамперед цей напрямок. Вашим водієм може бути один з ваших охоронців, але принаймні він повинен бути навчений агресивній манері водіння. Водій повинен регулярно тренуватися виконанню маневрів в умовах симуляції нападу на той випадок, щоб він не завмер на місці й міг адекватно реагувати, якщо відбудеться дійсний напад.

Якщо вас супроводжує ще одна машина з охоронцями, водій цього автомобіля повинен завжди намагатися зупинити свою машину між вашою й будь-якою потенційною погрозою. Якщо ви виявилися в тупику й уперед немає проїзду, а снайпери перебувають по обидва боки дороги, другий автомобіль повинен з'їхати з дороги для того, щоб дати вам можливість виїхати й прикривати, при цьому, вогнем ваш відхід. По приїзду на місце з машини першим повинен вийти охоронець для того щоб оглядітися. Тільки після того як він вирішить, що все в порядку, він може відкрити двері, прикриваючи вас своїм тілом.

Обережність. Ваші охоронці повинні бути завжди обережними й не особливо говіркими, особливо серед ваших друзів і ділових партнерів. Публіка зачарована зброєю й таємничим характером роботи охоронців. Ваші охоронці повинні ухилятися від відповідей на питання про свою роботу. Вони ніколи не повинні ні з ким обговорювати питання їхньої роботи на вас й особливості вашої охорони й вуж тим більше добровільно розповідати про свою роботу.

Їхня роль полягає в тім, щоб їх бачили, але не чули. Вони не є гостями на вашій вечірці або діловій зустрічі, вони перебувають там тільки з однією метою - забезпечити вашу безпеку. Вони не повинні говорити кому-небудь, що вони працюють на вас або намагатися зав'язати контакти на вашій діловій або розважальній вечірці. Звільняйтеся від охоронців, які намагаються бути з вами занадто фамільярними або починають ставитися до вас, як до приятеля, а не роботодавцеві. Це може бути винятково небезпечно.

Один покійний латиноамериканський політик наполягав, щоб його охоронці пили й ходили до жінок разом з ним. Їх же робота полягала в охороні цього політика, а не в участі в розвагах разом з ним. Подібним чином одна відома голлівудська зірка настояла на залученні свого охоронця в бізнес, а один з них був названий асистентом режисера одного з фільмів. Людина, що думає про справи, навряд чи має час або навіть намір думати про надійність безпеки свого наймача.

Здоровий глузд. Охоронці не зроблять вас невидимим. Ваша безпека ще багато в чому залежить від вашого здорового глузду. Не треба понапрасну ризикувати тільки тому, що у вас є охоронці. Багато з людей були вбиті або викрадені після того, як їхні охоронці були знищені терористами. Приведемо один факт, відомо що Альдо Морро, лідер Християнських демократів, мав охоронців, але це не врятувала його від рук членів Червоних бригад.

Постійне тренування. Є три слова, які мають безпосереднє відношення до вашої охорони: 1.) - тренування,

2.) - тренування

3.) - й ще раз тренування.

Ваші охоронці повинні постійно прагнути до вдосконалювання за допомогою тренувань. Вони повинні щомісяця мати час для тренування по стрілянині, ознайомлення з новими даними про з й інші потенційні погрози, на вивчення мов і бути в курсі всіх нових досягнень в області охоронної технології. Вони повинні тренуватися в умовах симуляції реальних подій. Періодично ви повинні присвячувати один із днів обговоренню дій зі своєю охороною на випадок можливого викрадення або нападів. Працюючи один з одним у тісному контакті, ви навчитеся попереджати дії один одного, тому, якщо виникне дійсна проблема, у вас не виникне питань як треба діяти з урахуванням вашої безпеки.

Таємні служби США

Самі елітні із них - ФБР(Федеральне Бюро Розслідувань), ЦРУ (Центральне Розвідувальне Управління), АНБ (Агентство Національної Безпеки) і, нарешті, "Сикрет Сервіс". Всі вони так чи інакше забезпечують охорону секретних державних об'єктів - атомних електростанцій, монетних дворів, банківських сховищ, вузлів зв'язку різні підприємства і ВІР - персон.

На професіоналів особливого роду, так названих секьюриті, покладена функція охорони ВІР-персон - президента країни, його найближчого оточення, директорів найважливіших державних служб, установ, міністрів, послів і т.п.. Залежно від категорії охоронюваних персон й об'єктів, а також від досвіду й кваліфікації, агенти спецслужб одержують від 60 до 80 тисяч доларів у рік.

Всіх секьюриті в США ділять на три основні групи: професійні охоронці й особисті охоронці із спецслужб, поліцейські - професіонали й особисті (часні) детективи. Сама численна з них група - поліцейські. Їх наймають, коли організації або якійсь особі потрібно перевезти коштовний вантаж, важливі документи, гроші, коштовності або забезпечити безпеку людини, на чиїй совісті немає порушень закону. У цьому випадку поліцейському платять від 180 до 220 доларів у день. Що стосується приватних охоронців, те їхня оплата прямо залежить від значимості охоронюваної персони й ступеня ризику.

Втім, послуги професіонала, подібного зіграному Кевином Костнером у фільмі "Охоронець" (а такий володіє не тільки професіоналізмом і досвідом, але й винятковим, неправдоподібним чуттям на небезпеку), оцінюються в 3-3,5 тисячі доларів у тиждень. Саме таким довіряють свою охорону зірки Голівуда, знамениті спортсмени, боси великого бізнесу.

Четверо охоронців Підлоги Маккартни, наприклад, одержують під час його гастролей по 375 доларів у годину. Приблизно стільки ж платять своїм охоронцям Мик Джаггер, Мэрайя Кэрри, Уитни Х'Юстон, Деми Мур, Клаудиа Шиффер, Леонардо ДИ Каприо, Джордж Клуні.

Серед приватних детективів, найманих для охорони торжеств і розважальних вечірок, як правило, чимало знаменитих спортсменів. Це борці й боксери, майстри єдиноборств і стрілки. Всі вони проходять річне навчання в спеціальних школах і платять за науку від 600 до 1000 доларів у тиждень залежно від престижності школи. Двічі в рік для них проводять обов'язкові семінари по перепідготовці, які в жодному разі не можна ігнорувати, інакше ти не зможеш розраховувати на добре оплачувану роботу.

Охоронцям великих бізнесменів платять до 400 доларів в годину, але потрапити в цю еліту надзвичайно складно. Як правило, вони живуть у будинку наймача й працюють практично цілодо-бово . Хазяї навіть відводять їм місце у своєму заповіті на правах члена родини. Іноді отримана спадщина становить таку суму, який він не заробить за все життя. Однак у випадку серйозного "проколу" охоронець назавжди губить репутацію. І тоді йому краще перекваліфікуватися.

7.4. Газова зброя в умілих руках

Ставлення до газової зброї в суспільстві неоднозначне й, як правило, зневажливе в цьому відношення. Власники газових балончиків часто люблять повторювати, яку гидоту вони купили, власники газових пістолетів ховають їх від сторонніх очей подалі. Зв'язано це в першу чергу з тим, що злочинці рідко бояться таких засобів захисту і продовжують нападати в момент їхнього застосування. Але причини також криються й у самих власниках газової зброї. Їхня проблема не в тім, що зброя слабко або неякісно, а в тім, що вони просто не вміють ним користуватися.

Газові балончики

Почнемо із застосування газових балончиків. Їхня ефективність залежить у першу чергу від спритності й сміливості того, у кого балончик у руках. Що стосується технічних характеристик, те не всі так погано. Газові засоби самооборони мають право на існування, і обвинувачувати балончик у неефективності проти 10-15 чоловік з відстані 4-5 метрів при морозі -30°С не зовсім правильно.

Балончик розрахований на застосування максимум проти двох нападаючих з дистанції 0,5-1,5 метра при температурі не менш -10°С и незначному вітрі. Що стосується охоронця, що застосовує балончик, то він повинен мати серйозну вправність і не думати, що тільки наявність одного балончика його захистить. Варто завжди пам'ятати, що після вдалого застосування газового балончика проти нападаючих потрібно правильно оцінювати свої сили.

Якщо нападаючі міцні, їх трохи - через якийсь час дія газу пройде й вони знову нападуть. Самим грамотним у цьому випадку буде – напасти

самому ще до цього моменту. Адже, по-перше, при повторному застосуванні газ у деяких балончиках діє слабкіше, а по-друге, було б нелогічно намагатися затримати агресивно настроєних до вас злочинців, маючи в арсеналі всього лише той самий балончик. Вони про це теж - вже знають, що їх чекає, тому постараються вас знешкодити, не потрапляючи під дію газу.

Більшість людей не враховують цих факторів, намагаючись затримати злочинців самостійно. У результаті попадають у переробку серйозніше, ніж було спочатку, тому що тепер нападаючі хочуть ще й помститися. Тепер вам необхідно врахувати температурний режим.

Що стосується температурних режимів, те тут теж потрібно бути уважним. У сильну жару газ більше розріджений й, відповідно, дія його слабкіше; у холод навпаки - балончик може змерзнути й газ розпорошуватися не буде.

Газовий балончик потрібно купувати в спеціалізованому магазині, знати особливості його дії при різних температурних режимах і навчитися застосовувати, завжди тримаючи в легкодоступних місцях. Можна також додати, що варто враховувати напрямок вітру, але це дурості з інструкції, тому що в екстремальній ситуації ніхто ніколи цього не враховує. Тому постарайтеся балончик максимально близько наблизити до очей нападаючі й уже потім нажати.

Газові пістолети

Для приклада візьмемо газовий пістолет BLOW COMPACT MOD.2002 BLACK PISTOL.

З газовими пістолетами всі набагато складніше. У деяких злочинців прямо камінь із душі падає, коли вони довідаються, що у вас не вогнепальний пістолет. А ще й на рожен лізуть більш упевнено, начебто у вас і зовсім ніякого захисту немає. Тому найважливіше правило при застосуванні такого пістолета: вихопив - стріляй.

Принцип дії

Принцип дії газової зброї трохи схожий із принципом дії його вогнепального побратима. Воно також споряджається унітарними патронами й у точності копіює механізми тих моделей, копією яких є. Але стріляє газова зброя не кулею, а газоутворюючим зарядом, що складається з активної порошкоподібної речовини й "вишибленого" порохового заряду.

Пострілом називається викидання заряду, у цьому випадку аерозольного струменя, з каналу стовбура газової зброї тиском порохових газів, що утвориться при згорянні порохового заряду. Заряд пороху, або

його еквівалента (ТЕРЕН-3 заряджений таким от еквівалентом, рецептура якого зберігається в строгій таємниці), згоряючи, перетворюється в гази з дуже високим тиском і високою температурою.

Під впливом температури й тиску кристалоподібний порошок активної речовини переходить із твердого стану в газо-аерозольну хмару й викидається під дією тих же порохових газів на відстань, що залежить від калібру зброї й боєприпасів, а також від пристрою розсікателя.

Відстань до супротивника

До відома, постріл в упор з газової зброї може нанести поранення з необоротними наслідками для організму людини. Гідродинамічний струмінь на відстані до 10-20 сантиметрів може нанести важке поранення, сполучене з опіком і влученням разом з елементами пластикового пижа в рану аерозольного струменя газового заряду, що викликає інтоксикацію організму (отруєння).

Що стосується далекобійності газової зброї, те поширена омана, що залежно від довжини стовбура дальність пострілу обчислюється до 7 метрів. Це в принципі вимисел, однак існує такий газовий пістолет-кулемет болгарського виробництва "Булфос", до речі перший з відомих газових пістолетів-кулеметів, і він дійсно має радіус поразки до 7 метрів, але при одній умові - якщо зарядити в обойму газові й холості патрони через один, що дозволяє зробити подвійний "удар" порохових газів і забезпечує цієї моделі збільшену зону дії.

Однак це не грає особливої ролі у вражаючій здатності цього виду зброї, тому що вже на відстані 5 метрів концентрація газової хмари зменшується настільки, що не має такого дії, щоб зупинити противника, як, скажемо, на відстані 3-4 метра.

Справедливості заради потрібно помітити, що, по статистиці, вогневий контакт із застосуванням коротко ствольної вогнепальної зброї відбувається на відстані від 5 до 10 метрів. Так що розчарування із приводу малої далекобійності газової зброї в цьому випадку недоречно, Ви ж не зі снайперської гвинтівки збираєтеся стріляти по нападнику.

Наявність у конструкції газової зброї передбаченої для стрілянини сигнальними ракетами, ці насадки робить газовий пістолет більше багатофункціональним, що дозволяє використати його не тільки як зброю самозахисту, але і як сигнальне застосовуване, наприклад, як для відлякування диких тварин, так і для стрілянини сигнальними ракетами, коли заблудилися у лісі, або у горах.

До речі сказати, газова зброя - досить ефективний засіб самозахисту від собак, щоправда, для цього підходять не всі патрони, а тільки зі змістом капсаіціна. В основному вони мають червоне маркування, тільки не плутайте з Тереном-3. Хоча він у принципі теж придатний для захисту від собак. Якщо ж це бродячі собаки, то отут досить холостого пострілу, для того щоб вони відстали.

Способи застосування

Є стійка думка, що застосовувати газову зброю в приміщенні не можна. У принципі це неправда, якщо дотримуватися декількох перевірених правил, можна дати відсіч й у закритому приміщенні газовою зброєю, при цьому мати мінімум втрати. Наприклад, постріл холостим патроном в упор через одяг наносить травму, сумісну з наслідками сильного удару куркулем, (від удару кулаком, нападник швидко отямиться, а при пострілі - у нього залишаються синець завбільшки з долоню й опік, аж до легкого поранення у живіт осколками пластмасового пижа, ну й плюс шоковий ефект).

Але врахуйте: постріл газовим патроном в упор може нанести важке поранення з інтоксикацією організму. А струмінь газу, відбившись від Вашого супротивника, може рикошетом уразити Вас.

Не так давно стався випадок, коли таким пострілом був убитий підліток.

Був ще один цікавий випадок, описаний одним зі членів стрілецького клубу. Він спостерігав, як на перехожого напав розлютований пес без намордника й повідця. Перехожий не злякався, вставив газовий револьвер у вухо розлюченого ротвейлера й зробивши два постріли газовими зарядами. Правда хлопець сам нахапався свого газу, а от собака здохла від ран, несумісних з життям.

Газова зброя цілком придатна для оборони своєї квартири або охоронюваного приміщення, якщо дотримуватися декількох правил. Якщо "ломляться" до Вас у квартиру нападники, відкрийте двері на ланцюжку й зробіть кілька пострілів у щілину між кістяком і дверьми, після чого захлопніть їх. Ваші супротивники напевно, коли йшли "на справу", протигазів з собою не брали і тому не захочуть далі ломитися у ваші двері в такій газовій хмарі.

Тільки після того як Ви захлопнули двері, постарайтеся відійти від дверей у бік, тому що є ймовірність пострілу у відповідь уже з бойової

зброї у двері, після чого супротивник у більшості випадків намагається зникнути з місця пригод.

Якщо грабіжники напали на охоронюване Вами приміщення й умудрилися проникнути усередину, саме головне - не панікувати, а відступаючи вглиб приміщення, декількома пострілами з газової зброї створить за собою - газову хмару. Злочинці не кинуться на хмару, а постараються його обійти, так що стріляйте кілька разів, щоб "загазувати" приміщення й не дати їм переслідувати.

Після чого покиньте загазоване приміщення, при цьому постарайтеся затримати подих і вискочити в сусідню кімнату, щільно закривши двері й забарикадувавшись. Потім викличте міліцію. Якщо в приміщенні присутній сльозоточивий газ, довго Ваші переслідувачі тримати облогу не будуть.

При покупці газової зброї, постарайтеся вибрати пістолет з більшим обсягом магазину. Це викликано необхідністю робити більше одного або двох пострілів по супротивнику для його повної нейтралізації. Якщо ж Ви придбали револьвер або пістолет з обмеженою кількістю патронів у магазині, допустимо 7, 8 і т.д., подбайте про придбання додаткової обойми для пістолета або так називаного "прискорювача" для револьвера. Повірте, це для Вашої ж безпеки! Наголошуємо, що ефект від застосування "газовика" не можна порівняти з дією бойової зброї, але це, вже окрема тема, яка буде викладатися на семінарських заняттях.

Якщо ви постраждали від дії газової зброї

Якщо все-таки Вам сильно "дісталося", то для швидкого усунення наслідків - можна застосувати п'ятипроцентний розчин харчової соди або борної кислоти (приблизно одна чайна ложка на склянку води). Правда, борна кислота може в деяких людей викликати алергійну реакцію, тому після знезаражування необхідно умитися більшою кількістю води з-під крана. Однак при сильних поразках навіть після надання першої допомоги необхідно доставити потерпілого до лікаря, де йому буде надана необхідна медична допомога.

7.5. Бронежилет - як засіб індивідуального захисту

Різко зросла міць вражаючих елементів з поширенням вогнепальної зброї у військовій справі привела до того, що збруя й панцири вийшли із уживання - вони перестали бути перешкодою для куль і тільки обтяжували своїх власників. У протистоянні засобів індивідуального броне захисту (СИБ) і вражаючих елементів - перевага завжди буде залишатися за останніми.

Адже якщо енергія, надана кулі, снаряду і відповідно до його конструкції може збільшуватися й змінюватися для досягнення своєї потужності й ефективності, то що тоді можна вдосконалити, щоб зробити менш уразливою людину – як можна модернізувати її захист.

Не тільки вдосконалювання техніки й створення нових матеріалів дозволило, (згодом засобам захисту,) наблизитися до рівня розвитку засобів небезпеки й знову зайняти своє місце в екіпіруванні бійця. Досить істотне, якщо не вирішальне, значення в цьому змісті має тактика війн.

На певному етапі Першої світової війни - а саме до цього часу відноситься початок відродження СИБ - воюючі сторони перейшли до позиційної війни, армії зарилися в землю, відсоток втрат у живій силі від артилерійського вогню різко зріс. Французька армія першої прийняла на озброєння сталеві шоломи, що стали відомими як каски Адріана обр. 1915 р.. Почали розробляти перші конструкції бронежилетів (БЖ), вони мали багато недоліків.

Незалежно від типів і конструктивних особливостей жилетів, великим мінусом - є маса, збільшення якої прямо пов’язане з підвищенням захисних властивостей БЖ, а також те, що жилет не забезпечував захист всієї поверхні тіла. Крім того - ступінь захисту прикритої жилетом поверхні не завжди одноманітний (диференційований захист). Навіть бронекостюми саперів-підривників, повністю перекриваючи фронтальну проекцію людини, не розраховані на аналогічний захист зі спини. При цьому рухливість людини знижується до рівня водолаза, що крокує у важкому костюмі по морському дну, а для забезпечення подиху й відводу тепла необхідно застосовувати спеціальні міри.

Армійський бронежилет (загальновійськовий, не спеціальний) прикриває на тулубі бійця проекцію найбільш важливих органів і забезпечує захист тільки від якогось (обумовленого при створенні БЖ) ряду вражаючих елементів, енергія яких при зустрічі з перешкодою не перевищує

певний (заданий) рівень. Додатково жилет може бути оснащений стоячим коміром для захисту шиї (у тому числі й від рикошетів від основного захисного пакета) і доповнюватися паховою панеллю (остання може бути знімної).

Захисними елементами в сучасних бронежилетах є багатошарові пакети зі спеціальної тканини (кевлар, ТСВМ) і броне пластини, (спеціальні сплави на основі титану, марганцю, кераміки й т.д.). Жилет може бути "м'яким" - при використанні тільки пакета захисної тканини. Такий жилет захищає від низькоэнергетичних вражаючих елементів - звичайних куль пістолетних і револьверних патронів невисокої потужності, холодної зброї. М'який жилет може бути посилений додатковими бронепластинами, що збільшує його захисні властивості.

Для захисту від могутніших вражаючих елементів - осколків і куль із більшою кінетичною енергією - конструкція жилета виконується твердою, її основою є бронепластини в сполученні з пакетом захисної тканини. Найбільш важкі захисні (балістичні) пакети здатні протистояти звичайним кулям сучасних автоматів (штурмових гвинтівок) під патрони 5,45 х 39, 5,56 х 45, 7,62 х 39 при стрілянині із близьких дистанцій (десятки метрів). Захистити від бронебійних куль гвинтівко-кулеметних патронів при стрілянині із близької відстані практично жоден сучасний БЖ не в змозі. Це межа для бронежилета, тому що крім зрослої маси жилета, імпульс від поглиненої енергії стає непосильним для людини.

Типи й характеристики вражаючих елементів, на протистояння яким розрахований БЖ, визначають клас захисту БЖ. Це - основна характеристика БЖ й одночасно найбільш складний параметр, що є наріжним каменем у суперечках і основною причиною плутанини в класифікаціях БЖ і віднесенні конкретного зразка до певного класу захисту. Дотепер немає єдиної системи класів захисту БЖ.

Наприклад, по класифікації НАТО жилети ділять на чотири класи захисту, де перші два протистоять кулям пістолетних (револьверних) патронів при стрілянині з пістолетів (револьверів) і пістолетів-кулеметів, два останніх - осколки різної енергетики, звичайним і спеціальним кулям автоматів (штурмових гвинтівок). Класи прийнятий позначати римськими цифрами. Крім того, практикується розширення класів на підкласи, з додаванням прописних латинських букв (a, b), а іноді й кількість класів збільшують до шести. Іноді рівень захисту позначають, безпосередньо вказуючи патрони, від куль якого БЖ здатний захистити, і тип куль.

Але подібні поділи БЖ ніколи не можуть бути конкретними, і безпечними до певного ступеня захисту. Куля патрона 5,45 х 39 з термоміцним сердечником значно перевершує по пробивній дії таку ж кулю з не термоміцним сердечником, ще більшу бронепробиваємість має куля ПП (підвищеної пробивальності) із загартованим спеціальним сердечником, і тим більше - куля БП (бронебійна). Все це - у межах одного патрона, при одній і тій же дуловій енергії.

Але розширювати класи захисту, розписуючи їх по кожному типі кулі (кожного патрона) - не представляється можливим.

Тому найбільше раціонально визначення, що загальними є 4 - 5 класа, кожен конкретний зразок БЖ характеризуючи додатковим точним технічним описом. Але це окрема тема. І як ми можемо віднести конкретний БЖ до таких загальних категорій, як "армійський", "протиосколочный" і т.д., настільки важко сказати, від якої конкретно кулі він здатний захистити, при яких умовах стрілянини, з якої дальності, і які будуть наслідку цього захисту.

Наприклад, кулі пістолета ПМ (патрон 9 х 18) і пістолета ПСМ (патрон 5,45 х 18) поводяться при зіткненні з багатошаровим захисним пакетом ТСВМ (тканина спеціальна високомолекулярна - вітчизняний аналог кевлара) по-різному. При приблизно одній і тій же питомій енергії й в 2,5 рази меншої дулової енергії куля пістолета ПСМ за рахунок завуження головної частини здатна розсовувати волокна й проникати на велику глибину. Тоді як куля пістолета ПМ внаслідок сферичної форми головної частини надійно зупиняється тим же пакетом ТСВМ.

Енергія удару рукою або багнетом перебуває в межах 8-10 кгм, енергія удару кулі автоматного патрона 5,45 - 7,62 мм - 150-200 кгм, кулі кулеметного патрона - у середньому 350 кгм. Крім стійкості балістичного пакета до пробиття кулею, другим, настільки ж істотним критерієм є запреградна дія кулі, що виражається в ступені контузії (тупої травми). На ранніх етапах конструювання жилетів цьому приділялося зовсім мало уваги. Потужні удари боксерів-важкоатлетів, що відправляють супротивників у нокдаун - це тільки одна - двадцята тієї нищівної сили, що куля автомата або гвинтівки здатна передати корпусу людини при стрілянині із близької дистанції. При такому влученні боєць, незалежно від типу бронежилета й особистих фізичних даних, у кожному разі безумовно виводиться з ладу. Чи буде ця втрата поворотної, або людина залишиться інвалідом

або навіть загине - залежить не тільки від кулестійкості жилета, але й від пристрою запреградної системи, що амортизує.

Чохол жилета - тихорєцька основа, що служить для розміщення балістичних панелей і формуючий зовнішній вигляд жилета - може забезпечуватися кишенями для перенесення магазинів, гранат, інших елементів озброєння й оснащення, сполучаючи в такий спосіб функції розвантажувального жилета. Розміщений на жилеті боєкомплект може в ряді випадків служити додатковим захистом. Але до цього питання підходять дуже обережно, як взагалі до розташування, кріпленню, матеріалу й конструкції фурнітури жилета. Справа в тому, що не тільки частини куль, що деформувалися, але й осколки балістичного пакета й будь-які частини, зірвані при влученні кулі або осколка, можуть рикошетом уразити бійця в будь-яку відкриту частину тіла.

У роки ВОВ для потреб Радянської Армії виготовлявся сталевий нагрудник СН-42. Але в той час БЖ в арміях широкого застосування й поширення не мали, та й бронежилетів у сучасному розумінні тоді не було. У спеціалізованій літературі згадується жилет під індексом 6Б1, що надійшов на постачання СА в 1957 році. Жилет тоді мав перекриваються бронепластини із спеціального сплаву, на ватяній підкладці.

При потужному науково-технічному потенціалі, залученому у військову галузь, загальновійськові бронежилети (у сучасному розумінні) у Радянській Армії з'явилися пізніше, ніж в арміях інших країн. Тому причиною відомі пріоритети, що ставили людське життя на останнє місце. Життя солдата в тоталітарній державі була й залишається самою вигідною, ходовою розмінною монетою.

Першим серійним загальновійськовим жилетом, прийнятим на постачання СА на сучасному етапі став протиосколочний жилет Ж-81 (індекс виробу - 6Б2) зразки 1981 р. По всій імовірності роботи в цьому напрямку були значною мірою стимульовані розгортанням Афганської війни. Балістичний пакет Ж-81 включав тоді перекривающі бронепластини товщиною 1,25 мм (у деяких джерелах - 1,4 мм) і 30 шарів тканини ТСВМ. Маса жилета - 4,8 кг. Жилет протистояв осколкам масою 1 м, що летять зі швидкістю 1000 м/с. Автоматні кулі пробивали жилет уже з дистанції 400-600 м.

В 1985 р. приймаються на постачання противокульні жилети Ж-85Т (6Б3-01) і Ж-85ДО (6Б4-01). У Ж-85Т використалися титанові бронепла-

стини товщиною 6,5 мм, у Ж-85ДО - керамічного бронепластини з карбіду бора. Обидва типи жилетів забезпечували диференційований захист:

- грудна секція - протикульний,
- спина секція - протиосколочний.

Це дозволило знизити вагу жилетів до 7-8 кг - попередні експериментальні жилети 6Б3ТМ й 6Б4 важили 10,5-15,5 кг.

В 1986 р. прийнятий на озброєння новий зразок - уніфікований бронежилет Ж-86 (індекс виробу 6Б5), що має дев'ять модифікацій (Ж-86-1, Ж-86-2, -3, і т.д.) і забезпечує відповідно різні рівні захисту й різну конфігурацію диференційованого захисту.

Жилет оснащений стоячим коміром для захисту області шиї. На чохлі жилета зовні розміщені кишені для автоматних магазинів й інших елементів озброєння. В області плечей передбачені валики, що перешкоджають сковзанню рушничного ременя із плеча.

Проблеми безпеки бізнесмена. Чи потрібний бізнесменові пістолет?

Законодавство дозволяє громадянам використати для самозахисту пневматична й газова зброя. На перше не потрібно ніякого дозволу. Але й користі від нього ніякого. Це іграшка. На друге потрібно одержати "добро" у міліції. Правда, дане відомство зробило все від нього залежне, щоб відбити бажання звертатися за відповідним документом. Але якщо ви терплячі, енергійні, наполегливі, не звертаєте увагу на такі дріб'язки, як хамство чиновників у мундирах, їх, м'яко говорячи, формалізм і глибоку до вас ворожість, то в кінців-кінців, через місяць або два щоденні зусилля ви одержите необхідний папірець. І зможете тоді купити газову "гармату", точну копію бойової моделі. Швидше за все, це буде "маузер", "Вальтер" або який-небудь інший зразок славної збройової промисловості Німеччини. Ціни для богатих більш ніж доступні: 200-300 дойчмарок, хіба це гроші?

От отут і виникає питання: яка вам від газового пістолета (або револьвера) користь?

Ми висловлюся по даному приводі різко: користь майже нульова, шкода дуже великої. Справа в тому, що коли ви дістаєте з кишені або кобури свою незабійну зброю, зовні воно виглядає точно так само, як "сьогодення", бойове. Отже, будь-який злочинець вирішить (і чисто технічно буде цілком прав), що ви зібралися його пристрілити. Отже, йому не залишиться нічого іншого, крім як застосувати свою зброю першим

(вистрілити, метнути ніж, збити з ніг, нарешті). Після цього ви вже не зможете йому довести, що хотіли всього-на-всього "залякати ", а не калічити й, тим більше, не вбивати.

Запам'ятаєте: газова зброя в руках що обороняється провокує злочинців на більше рішучі й жорстокі дії.

Що стосується вражаючих характеристик, то вони в газової зброї вкрай низькі. Особливо на відкритому повітрі, де газ стрімко розсіюється, і де відбувається більшість нападів на бізнесменів.

А в закритому приміщенні, відбившись від стіни або від меблів, газова хмара діє на стрілявшого не гірше, ніж на той, у кого він цілив. Не випадкове застосування газової зброї в закритих приміщеннях заборонено інструкцією МВС.

Сказане нами розуміють не всі. Тому вони прагнуть обзавестися "дійсною зброєю", наприклад, пістолетом "ТТ" (хоч і стара система, але непогана), "Макаровым" або чеським ЧЗ-85 (дуже гарна машинка) і т.д. Що ж, гарний пістолет тим і гарний, що з ним мимоволі почуваєш себе якось затишніше й спокійніше. Забуваєш навіть про те, що придбав його й носиш при собі зовсім незаконно. Втім, ми реалісти. Нам зрозумілі міркування начебто такого: "раз міліція захищати нас не може й не хоче, доводиться рятувати себе самим".

Поговоримо про інше, застосування зброї.

Розглянемо випадки, коли стрілок з пістолета здатний використати його з належною ефективністю? Фахівці давно це сформулювали. Насамперед , відзначають вони, верх божевілля тримати свою зброю про запас, на випадок нападу, де-небудь у ящику стола, в аташе-кейсі або внутрішній кишені піджака. Навіть у художніх фільмах, досить далеких від правди життя, персонажам украй рідко вдається вчасно витягати пістолет з подібних місць. У реальній дійсності подібна можливість взагалі виключена, адже грамотний напад відбувається стрімко, раптово, у самий невідповідний момент.

Ми вже згадували, що нальоти досить рідко відбуваються у квартирі й на роботі. Звичайне місце для них - дорога туди або назад. Іншими словами - на повітрі. Чи вмієте ви стріляти не в тирі, а під відкритим небом? З із положення, наприклад, сидячи або лежачи? Під вогнем - у вашу сторону? По людям, нехай навіть злочинцям? По мішенях, що рухаються в різних напрямках ",", у тому числі по тим, хто біжить до вас?

Щоб все згадане стало для вас можливим, необхідно щодня, (підкреслюємо, щодня) як мінімум тридцять хвилин (краще година) приділяти тренуванню по вихоплюванню пістолета відтіля, де він у вас перебуває, і прицілюванню в мішень. Спочатку мішень може бути нерухомої, однак максимум через місяць варто перейти до прицілювання навскидку по мішенях що рухається. Ролі таких мішеней можуть виконувати свійські тварини (кішки, собаки, птаха), члени родини, товариші по службі, перехожі. В останньому випадку треба бути вкрай обережним, інакше справа може скінчитися дуже неприємно для вас. Найкраще щодня відвідувати спеціально обладнаний тир, якщо такий є. Як би там не було, якщо ви не розів'єте в себе навичка миттєвого вихоплювання пістолета й точного наведення його на мету по стовбурі в спокійній обстановці, то в екстремальних умовах у вас свідомо нічого не вийде.

Необхідно також не рідше двох разів у тиждень стріляти зі свого пістолета. Саме зі свого, тому що особиста зброя обов'язково повинне бути пристріляне власником. Число пострілів за тренування від 10 (мінімум) до 30 (максимум). Задоволення не з дешевих, адже один патрон коштує приблизно долар. Стрілецькі вправи треба час від часу ускладнювати. Наприклад: за 6 секунд уразити 5 мішеней, розташованих віялом перед вами на видаленні від 5 до 25 метрів. Або потрапити в три мішені, що рухаються на вас із різного видалення й з різною швидкістю.

Нарешті, у влучного стрільця повинна бути тверда рука й вірне око. Отже, алкоголь (у більших дозах, або потроху,) але часто, нічні посиденьки, навіть сигарети снайперові протипоказані. Чи готові ви відмовитися від горезвісних "радостей життя" і щодня тренуватися заради того, щоб гарантовано застосувати зброю "на випадок чого"? Нам це здається більш ніж сумнівним.

Зробимо висновок: не тільки газове, але й бойова зброя дилетантові не допоможуть. У недотепних руках воно годиться винятково для того, щоб розмахувати їм перед носом іншого такого ж дилетанта. Ще можна лякати їм підлеглих, сусідів, членів родини, перехожих. Тому наша вам рада: залишіть зброю професіоналам, якщо ви самі не є таким.

Яким повинен бути охоронець

По логіці речей, професіоналами повинні бути охоронці. Наприклад, у Москві в охороні бізнесмена "середньої руки" іноді зайнято до 10 чоловік, що працюють у три зміни. Іншими словами, вони прикривають його цілодобово. У що це обходиться, точно ніхто не знає. Якщо виходити

з того, що середня російська зарплата на початок 2000 р. становила 250 доларів, то вже виходить не погана сума "зелених". Але ж тим, хто охороняє ваше життя, життя рідних і близьких людей, платити треба багато вище за середній рівень. Видимо тому більшість підприємців обходиться або без охорони, або наймає одного, максимум, двох чоловік.

Прагнучи до економії, вітчизняні бізнесмени використають своїх "хоронителів". Наймають охорону - багатофункціональну: і шофери вони, і посильні, і камердинери, і бог знає хто ще. Відразу скажу, що такий підхід найчастіше невірний. Простий приклад: у вас двоє охоронців в автомобілі разом з вами. Ви виходите, один з них відкриває вам дверцята, другий виключає запалювання й ховає ключі в кишеню. Секундна справа, але руки й очі в обох зайняті. Цих двох-трьох секунд цілком достатньо для того, щоб без усяких перешкод застрелити й вас, і їх. Спеціалісту середньої руки, вистачило б на даний захід півтори секунди.

Експерти єдині в думці, що навіть один-єдиний охоронець здатний уберегти клієнта від безлічі неприємностей, якщо він - професіонал. Правда, у тих випадках, коли за бізнесменом починають планомірно полювати інші професіонали, його шанси залишитися в живі різко знижуються. Проте , надійно "закрити" від кілерів можна - у принципі - будь-якого клієнта. Однак це вимагає цілої команди добре підготовлених фахівців, систематичної оперативної роботи, першокласних технічних засобів - тобто , коштує більших грошей. Мало кому по кишені мати "особисту гвардію" в 10-20 чоловік. Переважна більшість бізнесменів у країнах СНД і Східної Європи намагається обходитися не більш, ніж двома-трьома "хоронителями" свого тіла.

Якщо у вас один охоронець, то краще увесь час ходити з ним разом. Якщо ж їх у вас два, то перед тим, як входити в під'їзд, необхідно одного відправити перевірити всі сходові клітки. Відпрацювати всі необхідні в такому випадку – заходи. Непогано заздалегідь потурбуватися й про бронежилети для всіх.

Відкриємо вам невелику таємницю, скажемо, що переважна більшість замовлених убивств на Заході відбувається снайперами з великої відстані. Це в першу чергу розуміють ті, що за кордоном, і тому там дуже добре розвинена школа охоронців. І якщо у нас убивці віддають перевагу під'їздам, то на Заході охоронці в такій ситуації миттєво перетворюють кілера в решето.

Звичайно бізнесмени самі вирішують, кому довірити своє життя, здоров'я й матеріальне благополуччя. Тому треба, щоб вони орієнтувалися в проблемах, пов'язаних з особистою - "охороною тіла" більш відповідально..

7.6. Загальні міри захисту від замаху

Історія використання для охорони людини різних тварин настільки ж древня, як й історія людського суспільства. Як відомо, "гусаки Рим урятували" і було це за 390 років до початку християнської ери! Як сторожів виступали змії й з, отрутні павуки й скорпіони, барси й рисі, дикі кабани й очеретяні коти... За минулі століття стало ясно, що немає краще друга й захисника для людини, чим собака.

Ви самі знаєте, що собака – самий кращий охоронник, як у себе дома, так і на підприємстві.

Звичайно, мова не йде про милих цуциків, типу болонки або такси, що радісно кидаються на шию кожному, хто ввійшов у квартиру, що розчулено виляють хвостом побачивши кісточки в чужих руках. Ні, собаки повинні з добре дресировані спеціально для сторожової служби. У цьому випадку собакам з із по надійності й ефективності не має рівних: їх не підкупиш і не залякаєш, не застанеш зненацька. Вони менш уразливі, чим люди, більше живучі, більше агресивні. Собака вся, від морди до хвоста, являє собою живу зброю.

Собака - кращий друг бізнесмена

Чому ж, у такому випадку, вони досить рідко використаються бізнесменами для охорони? Відповідь проста: з ними багато метушні. Собак треба спеціально тренувати, годувати, вигулювати, лікувати. Все це вимагає часу, грошей, терпіння. І відповідних знань, тому що у використанні собак є ряд тонкостей, які обов'язково треба враховувати:

1.) Собака - жива істота, дуже розумне й емоційне. Обзаводячись собакою, ви берете на себе відповідальність за неї. Тільки закінчені покидьки здатні вигнати за двері свого друга, чия відданість обумовлена самою природою. У той же час тримати серйозного собаку для серйозних

цілей, не маючи для цього ні знань, ні грошей, ні часу можуть тільки несерйозні люди.

2.) Тому та людина, що буде відігравати роль провідника службового собаки (ви, хтось зі членів родини, ваш співробітник) обов'язково повинен пройти курс підготовки й провести дресирування собаки. Кваліфікованим є лише така тварина, що навчилося правильно діяти в екстремальних ситуаціях нападу. Це значить: воно вміє розпізнавати небезпеку, уміє атакувати збройних злочинців, уміє захищатися від них, кориться командам свого провідника.

3.) Собака повинна утримуватися в належних умовах. Так, її треба годувати 2 рази в день, основна їжа - вівсянка, зварена без солі, кілька мозкових кісточок і час від часу - консервований собачий корм із вітамінами й мікроелементами. Собаку має з годувати тільки одна людина, її провідник. Із чужих рук дресирований собака їжу брати не повинна. Неприпустима годівля сторожового собаки цукерками, ковбасою й іншими "людськими" ласощами.

4.) Собака повинна регулярно тренуватися в спеціально обладнаному місці: бігати, із через перешкоди, плазувати, нападати на опудало, на людину, що зображує злочинця, вислизати від наведеного на неї стовбура пістолета, рушниці, автомата, від петлі-зашморгу. Необхідно систематично розвивати в неї така якість, як "злість".

5.) Категорично забороняється бити собаку, репетувати на неї, тупотіти ногами, відбирати їжу, лізти до неї в п'яному виді, жартуючи нацьковувати на людей (собака жартів не розуміє), знущатися з неї (от глузування, як не дивно, собака розуміє дуже добре). Намордник варто одягати лише там, де це необхідно. Повідець повинен бути коротким і легко зніматися, щоб ваш захисник не міг зачепитися за який-небудь предмет.

6.) По своїй конституції (статурі) собаки розділяються на три основних типи:

- **важкі** (наприклад, доги, ротвейлери, чорні тер'єри),
- **середні** (наприклад, німецькі вівчарки, різеншнауцери, великі добермани),
- **легкі** (наприклад, ердельтер'єри, боксери, пітбультерьери).

Не вдаючись у дискусії, скажемо, що найбільш оптимальний варіант - це середній тип.

А найкращий собака - вівчарка або лайка, з тим застереженням, що вівчарка зліша, а лайка - розумніша.

7.) Є ряд "модних" порід собак. Це вбивці, спеціально використовувані для так званих "собачих боїв": пітбультерьери, стафордшири, великі доги. Всі вони надзвичайно агресивні, погано керовані, емоційно легко збудливі, тому - дуже небезпечні. У першу чергу для самих власників.

Уже відомо чимало випадків, коли ті ж пітбультерьери, образившись на хазяїна, нападали на нього сплячого й убивали. Ці цуцики запросто перекушують кістку руки, або горло у нападника.

І якщо тільки відчують, що хазяїн їх трошки побоюється, як моментально візьмуть ініціативу у свої руки. Тому в цивілізованих країнах таких собак або забороняють тримати в приватних житлах, або вимагають реєстрації в поліції й регулярних свідченнях про добромисне поводження.

Не рекомендуємо тримати для охорони собаку - колі, чия дурість загальновідома. Взагалі, сторожовий собака повинна бути розумна, слухняна, віддана, легко й високо стрибати, мати здорові гострі зуби, потужні лапи, сильний подих, широкі груди, короткий хвіст. Кастрація бойового собаки неприпустима.

8.) Основні варіанти атаки собак "середнього" типу полягають у стрибку на плечі, в ударі всіма чотирма лапами (або грудьми) у поперек, а також в ударі головою під коліна. Як тільки людина впала, собака пускає в хід зуби. Дресировані собаки вміють хапати за ноги, пах, плечі, горло. Особливо важливо виробити в собак рефлекс укусу за ту руку, що тримає зброю й нападати не тільки позаду або збоку (так надходять всі ненавчені собаки), але й попереду. Всі види атак необхідно відробити із твариною до повного автоматизму дій.

Методи дресури в цей час досягли високої досконалості, зупинка за малим - за тим, щоб робити це. На жаль, занадто часта справа не йде далі покупки породистої тварини, із прекрасного родоводу. Зважємо, що для сторожової служби зовнішній вигляд собаки, стан її тіла й психіки набагато важливіше всіх тих паспортів, нерідко "липових". Не будьте зайво довірливі, звертайтеся до фахівців саме в області застосування собак, і купуйте тварину тільки разом з ними. Не завжди буває, що найдорожча собака й її породистий папірець - найкращі . Занадто породисті тварини - це виродження виду, а не його розквіт. Вам звір (собака)потрібний для бою, не для конкурсу на найкрасивіший хвіст, модну зачіску та інше.

9.) У яких місцях собака може бути поруч із вами? У дуже багатьох: у квартирі, в офісі, на дачі, в автомобілі, у гаражі, під час прогулянки із

дружиною або з дітьми. Хіба що в театрі й у ресторані її присутність її - недоречна...

Загальні міри захисту від замахів

Вибух в офісі, у під'їзді, в автомобілі, у магазині став частиною повсякденного життя наших міст. Для прикладу візьмемо Росію, у Москві в 93-м року відбулося більше 300 вибухів гранат та вибухових пристроїв. У Санкт-Петербурзі ще більше. Результат - десятки вбитих і поранених людей, значний матеріальний збиток.

Арсенал злочинців досить різноманітний: від саморобних вибухових пристроїв до гранат Ф-1, РГД-5, протипіхотних і протитанкових мін. Усього два приклади найпростіших прийомів мінування: * - гранату Ф-1 (або зв'язування гранат РГД-5) прикріплюють до автомобіля, що стоїть в гаражі або на відкритій стоянці. У кільце чеки гранати просмикують волосінь, кінець якої прикріплений до нерухомого предмета за автомобілем. Машина починає рух, чека висмикується, граната вибухає. * * - Основні місця для мінування в машині, це сидіння водія, днище під передніми сидіннями, бензобак, капот. Значно рідше заряд вибухівки поміщають у багажник, у колісній ніші, під задні сидіння, в "бардачок" й інші місця.

Крім того, міна великої потужності може встановлюватися неподалік від автомобіля або в сусідній машині. Але в цьому випадку потрібне керування нею ззовні по радіо або підрив її за допомогою електричного проведення. Іншими словами, злочинець повинен перебувати неподалік від місця злочину й вести спостереження, що завжди вважається небажаним.

Ознаками, що насторожують вас, повинні служити наступні:

1 - поява якоїсь нової деталі усередині або зовні автомобіля;

2 - залишки пакувальних матеріалів, ізоляційної стрічки, обрізків проводів неподалік від автомобіля або усередині салону;

3 - натягнута волосінь, дріт, проведення, шнур, мотузка, так чи інакше прикріплена до будь-якої частини автомобіля;

4 - чужа сумка, коробка, валіза, пакет, згорток усередині салону або в багажнику;

5 - пакети, що з'явилися вже після паркування машини, з-під соків, молока, консервні банки, згортки, коробки й т.п. недалеко від автомобіля;

Залишаючи машину на тривалий строк без догляду (на ніч, на час роботи, на дачі й т.д.), хоча б навіть й в "надійному" гаражі або на охоронюваній автостоянці, використайте так називані "контрольки" на машині.

Це значить, що між крильми й капотом, на дверях салону, на кришці горловини бензобака, між сидінням і рамою треба приклеювати вузькі смужки липкої стрічки (ізоляційної, лейкопластиру, паперової й т.д.) під колір даної ділянки. Замість стрічечок можна приклеювати волоски, уламки сірників.

Якщо ця "сигналізація" виявиться порушеної, Ви не заводите машину, нічого не відкривайте в ній (наприклад, не намагайтеся підняти подушку сидіння) доти , поки не проведете ретельний візуальний огляд. У випадку виникнення підозр звертайтеся до фахівців-саперів. Необхідно також установити за правило, щоб машину обстежив, відкривав, заводив, розігрівав і торкав з місця хтось інший, а не ви. Цим "іншим" може бути ваш особистий шофер, охоронець, працівник що служить на автостоянки або кооперативного гаража, сусід по будинку.

Сучасні вибухові речовини, (типу радянського пластита, чехословацького семтекса) і засобу висадження - дозволяють фахівцям, що мають армійську підготовку, конструювати найрізноманітніші мініатюрні міни-пастки. На щастя, серед злочинців таких фахівців - мало. Тому злочинці застосують у більшості випадків кустарні вибухові пристрої.

Для замаху на бізнесмена може використатися й поштовий канал. Вибухові пристрої, що направляють у листах, використаються не для вбивства, а для лякання одержувача. Адже 20-40 грамовий заряд вибухівки може нанести, як правило, тільки поранення й викликати сильний шок.

Для знищення застосовують не листа, а бандеролі й посилки.

Вибухові пристрої, які закладають у конверти, бандеролі й посилки можуть бути двох напрямків, як миттєвого, так й уповільненої дії:

1.) Взриватели миттєвої дії виникають внаслідок спрацьовування вибухового пристрою при натисканні, ударі, проколюванні, знятті навантаження, руйнуванні елементів конструкції, просвічуванні яскравим світлом і т.д. Наприклад, вибухові пристрої, що діють за принципом музичної листівки, вибухають при їхньому розкритті. Вибухові пристрої в бандеролях спрацьовують або при відкриванні, або при спробі витягти книгу або коробку з упакування. Вибухові пристрої в посилках звичайно спрацьовують при розкритті кришки посилкового ящика.

2.) Взриватели вповільненої дії – спрацьовують після закінчення заздалегідь установленого строку (від декількох годин до декількох доби) викликають вибух, або ці взриватели приводять основний вибуховий

пристрій у бойове положення, після чого спрацьовування вибухового пристрою відбувається миттєво у випадку, коли хтось проведе зовнішній вплив на нього.

Однак, незалежно від типу взривателя й вибухового пристрою, листа, бандеролі й посилки з подібною начинкою неминуче володіють рядом ознак, по яких можна їх відрізнити від звичайних поштових відправлень.

Ці ознаки діляться на основні й допоміжні.

1.) До числа основних ознак відносять наступні:

- товщина листа від 3-х мм і вище, при цьому в ньому є окремі стовщення;
- зсув центра ваги листа (пакета) до однієї з його сторін;
- наявність у конверті предметів, що переміщаються, або порошкоподібних матеріалів;
- наявність у вкладенні металевих або пластмасових предметів;
- наявність на конверті масляних плям, проколів, металевих кнопок, смужок і т.д.;
- наявність незвичайного заходу (мигдалю, марципана, паленої пластмаси й інших);
- ”тікання" у бандеролях і посилках годинного механізму (один з найпростіших і розповсюджених взривателів роблять за допомогою звичайного будильника);
- у конвертах і пакетах, у посилкових ящиках при їхньому перекиданні чутний шорох порошку, що пересипається.

Наявність хоча б одного з перерахованих ознак (а тим більше відразу декількох) дозволяє припускати присутність у поштовому відправленні вибухової “начинки”.

2.) До числа допоміжних ознак ставляться:

- особливо ретельне закладення листа, бандеролі, посилки, у тому числі липкою стрічкою, паперовими смугами й т.д. ;
- наявність написів типу ”особисто в руки", “розкрити тільки особисто”,
- “вручити особисто”, “секретно”, “тільки директорові (власникові, голові)” і т.д. ;
- відсутність зворотної адреси або прізвища відправника, нерозбірливе їхнє написання, явно вигаданий адреса;
- саморобне нестандартне впакування.

З обліком сказаного, випливайте трьом обов'язковим правилам:

А. - всю пошту повинен розкривати тільки секретар, але не ви;

Б. - робити це треба в спеціально відведеному приміщенні подалі від вашого кабінету;

В. - у випадку одержання підозрілої кореспонденції секретар повинен вас інформувати, а вам треба вирішити, чи варто викликати фахівців.

Звертайте увагу на сторонні предмети, залишки ізоляції, про проводи й іншому, це має значення відносно офісу, квартири, дачі, під'їзду, навіть звичайних вхідних дверей, якщо тільки ви цими дверима користуєтеся систематично. Крім того, звертайте увагу на сліди ремонтних робіт, свіже фарбування (особливо окремих ділянок) стін і підлог, на перестановку меблів, на появу будь-яких нових предметів. Наприклад, 200 грам пластита неважко сховати в корпусі факсу, у квітковому горщику, у радіотелефонну трубку. Цих двохсот грамів пластита цілком достатньо , щоб автомобіль типу "Вольво" разом з усіма пасажирами перетворився в палаючий катафалк, а в кімнаті площею 24 квадратних метра не залишилося жодного живої людини!

Деякі міри загальної безпеки при замахах:

- уникайте виходити з будинку й офісу поодинці . Пересуватися в групі завжди безпечніше;
- намагайтеся, по можливості, уникати постійних маршрутів при поїздках на роботу й з її.

  Досвід показує, що злочинці звичайно тримають свою жертву під спостереженням, щоб вибрати найбільш підходяще місце й час для нападу. Виберіть хоча б 4 різних маршрути й користуйтеся ними за принципом випадкового вибору. Непередбачуваність - ваш кращий захист;
- намагайтеся їздити по жвавих дорогах, уникати пустельних вуличок і допоміжних доріг. Перевіряйте, чи не переслідує вас якийсь автомобіль. При русі по багаторядному шосе займайте місце в середньому ряді, щоб не дати можливості притиснути ваш автомобіль до узбіччя;
- коли їдете в машині, закривайте всі двері на кнопки, залишайте відкритим лише «вітровик» скла. Якщо вас зупинили (наприклад, ДАІ) не виходьте з машини, у всякому разі, якщо місце пустельне, а час доби темний. Машину тримаєте на передачі, щоб мати можливість у будь-який момент дати газ;

- якщо вам здається, що за вами стежать із іншої машини, перевірте це, раптово міняючи напрямок руху або швидкість, різко перебудовуючись із ряду в ряд і несподівані зупинки. Якщо в підозрілій машині злочинці, їм доведеться реагувати відповідним чином;
- якщо ваші підозри виправдуються, негайно зв'яжіться з міліцією або зі своєю власною "бригадою швидкого реагування". На цей випадок у вас обов'язково повинен бути радіотелефон, або «мобільник». Цей прилад не розкіш, а життєво важливий засіб безпеки й бізнесу;
- якщо машина зі злочинцями перегородила вам шлях (найчастіше в таких випадках використають "ножиці" - одна машина перекриває дорогу попереду, інша - позаду), на великій швидкості бийте в місце, що відповідає однієї третини машини злочинців,(відразу за переднім колесом або перед заднім). У жодному разі не зупиняйтеся. Якщо місцевість дозволяє, ідете на швидкості по узбіччю, по бездоріжжю;
- якщо злочинець готується стріляти по вашій машині, збільшуйте швидкість і направте автомобіль прямо на нього. Від куль укрийтеся пригнувшись нижче лобового скла, але продовжуючи тримати кермо руками в обраному напрямку. Збивши злочинця машиною, не витрачайте час на з'ясування того, у якому він стані. Негайно виїдьте на максимальній швидкості;
- необхідно, щоб всі місця в автомобілі (а не тільки передні) були постачені поясами безпеки. Бажано також зміцнити салон зсередини додатковим ребром жорсткості, що виключає сплющування у випадках падіння під укіс або тарана. Загалом кажучи, при бажанні автомобіль будь-якої марки можна за допомогою вмільців так обладнати для "війни на дорогах", що він стане свого роду "броненосним крейсером". І тоді ви зметете зі шляхи будь-який автомобіль, хто б їм не управляв;
- якщо в салон автомобіля закинули пляшку із запальною сумішшю, не зупиняйтеся. Температура усередині салону не здійметься вище 55-60 градусів, а така температура не буде небезпечною для життя. На граничній швидкості йдете від місця події - адже пляшку кинули саме для того, щоб "викурити" вас із машини. Якщо хочуть знищити, то кидають гранату типу Ф-1, а сам злочинець негайно ховається.
- Приїзд на роботу й від'їзд з роботи повинен бути різним за часом. Якщо можливо, з різними входами в будинок. Якщо вхід у ваш офіс тільки один, забезпечте постійний контроль за ним;

- Уникайте приїжджати в офіс у годину, коли там нікого немає. Остерігайтеся будь-якої сторонньої людини, без справи тиняючогося біля будинку або по коридорі. Жадайте від своєї охорони, з'ясування його особистості;
- Не стійте безцільно біля вікон. Не розташовуйте поруч із вікном своє робоче місце, якщо його можна переглядати з вулиці, з вікон (у тому числі з горища) найближчих будинків;

Запам'ятовуйте

1.) Ставтеся обережно до прохань про фотографування або інтерв'ю в себе будинку. Попередньо визначите час візиту, його тривалість, що ви дозволите сфотографувати або що скажете. На час візиту забезпечте себе охороною. Не впускайте більше число людей, чим це було обговорено заздалегідь. У кожному разі їх не повинне бути більше двох;

2.) Зробіть так, щоб ваші діти ходили в школу й зі школи в супроводі дорослих. Попередите вчителів, що ваших дітей ні за яких умов не можуть зустрічати й відвозити додому сторонні люди, у тому числі жінки;

3.) Виходьте завжди з того припущення, що ваш телефон прослуховується. Будьте дуже обережні в телефонних розмовах. Це стосується як службових телефонів, так і домашнього, а тим більше - радіотелефону;

4.) Попередьте рідних і близьких вам людей, щоб вони не впускали в будинок незнайомих, нікому не повідомляли відомостей про вашу діяльність, про місцезнаходження (крім офісу, розуміє), не приймали ніяких пакетів або предметів, якщо не знають, від кого вони прислані;

5.) Ставитеся насторожено до осіб, що видають себе за працівників міських комунальних служб, за ремонтників , за роздрібних торговців, що раптом з'явилися в районі вашого будинку або офісу (був випадок, коли вбивця замаскувався під вуличного продавця фруктів й установив свій візок поруч із будинком жертви. Бізнесмен вийшов з під'їзду й одержав кілька куль);

6.) Не обговорюйте плани ділових поїздок і зустрічей при сторонніх людях. Не ведіть ділових переговорів по телефоні в присутності відвідувачів. Якщо вам у цей час дзвонять, пропонуйте передзвонити пізніше;

7.) Підтримуйте дружні відносини із сусідами, особливо з літніми. Саме пенсіонери (особливо жінки), що проводять цілі дні на крамничках біля будинку, можуть першими вас попередити про підозрілі типи, про те,

що хтось цікавиться вами або вашою машиною, вашими дітьми, намагався проникнути у квартиру й т.д.;

8.) Обговорите з родиною, що вони повинні робити в тому випадку, якщо вас або когось із них викрадуть. Зробіть необхідні фінансові й інші розпорядження на цей випадок, укажіть декілька контрольних телефонних номерів. Розкажіть їм як і куди необхідно звернутися при необхідності, (територіальні правозахисні органи, оперативно-слідчі підрозділи, СБУ та інше.)

Якщо в такий момент ви опинилися на вулиці, і у вас не має грошей для дзвінка, не хвилюйтеся, подзвоніть в міліцію 0-2, в пожежну частину 0-1, або в швидку медичну допомогу 0-3 і пояснить ім. ситуацію, Ці служби прийдуть на допомогу, або порекомендують, що треба зробити в першу чергу.

Висновок

В заключення цього розділу, ми хочемо підкреслити, що незалежно від характеру погрози, або екстремальної ситуації, ви не повинні нічого робити поспіль. Керуйтеся наступними правилами:

- проаналізуйте саму екстремальну ситуацію, (погрози на вашу адресу);
- наскільки це можливо – «продіагностуйте» злочинця, визначте його фізичні і психологічні дані, настрій, поведінку;
- приведіть себе в той стан, при якому ви зможете думати і діяти, (як правило людина в такій ситуації впадає в « тормозну депресію « або навпаки – різко агресивна);
- зробіть оцінку ситуації і виробіть тактику і план дій з обліком на ваші обставини.

СЛОВНИК СПЕЦІАЛЬНИХ ТЕРМІНІВ

Агент - таємний співробітник розвідки або організації, що займається добуванням, вивченням й узагальненням відомостей економічного, науково-технічного, політичного, військового характеру про супротивника або конкурента.

Аналіз безпеки - розрахунок небезпек, пов'язаних зі здійсненням передбачуваної діяльності юридичної або фізичної особи.

Аналіз небезпеки - виявлення небажаних подій, що тягнуть за собою реалізацію небезпек, аналіз механізмів виникнення подібних подій й оцінка масштабу, і ймовірності будь-якої події, здатного зробити вражаючий вплив.

Апаратні засоби захисту - пристрою, системи й спорудження, призначені для захисту інформації від несанкціонованого доступу, копіювання, крадіжки або модифікації.

Апаратура інформаційного знімання це інформаційно-спеціальні, технічні засоби, призначені для одержання інформації шляхом прийому акустичних, електромагнітних, світлових, теплових або інших сигналів (випромінювань), що несуть оперативно значимі дані.

Апаратури технічної розвідки - сукупність технічних пристроїв виявлення, прийому, реєстрації, виміру й аналізу, призначених для одержання даних про об'єкт.

Афективний страх - найдужчий страх, викликуваний надзвичайно небезпечними, складними обставинами, що паралізує на якийсь час здатність людини до довільних дій.

База даних - сукупність організованих, взаємозалежних, збережених у пам'яті ЕОМ даних, що ставляться до певного обсягу або напрямку діяльності.

Банда: 1). Різновид злочинного співтовариства (об'єднання), що характеризується наступними ознаками: наявність мети й угод про спільну злочинну діяльність, розподіл

конкретних обов'язків на з угоди про спільну злочинну діяльність, озброєність. 2). Організована, збройна злочинна група, створена з метою нападу на підприємства, установи або на окремих громадян.

Бандитизм - один з найнебезпечніших злочинів, що зазіхають на основи суспільної безпеки й громадського порядку. Полягає в організації збройної групи (банди) з метою нападу на громадян або організації, а дорівнює керівництво нею, участь у збройній групі (банді) і в чинені нею нападах.

Банк даних - організаційно-технічна система, що включає в себе кілька баз даних і способи керування ними.

Банківські злочини - незаконні махінації й зловживання недосвідченістю широких верств населення. До цієї категорії злочинів ставляться: практика використання посадовими особами внутрішньої конфіденційної інформації в особистих інтересах, висновок незаконних спекулятивних угод або спонукання до них, емісія незабезпечених цінних паперів, надання помилкової або недостовірної інформації й здійснення інших дій, що створюють передумови для наступних злочинів.

Безпека інформаційної мережі - міри, що охороняють інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в нормальні дії або спроб руйнування її компонентів.

Безпека організації - стан її динамічної стабільності, у якій вона може здійснювати свої функції в повному обсязі. Стабільність характеризується динамічною рівновагою, балансом між впливом дестабілізуючих факторів і здатністю системи протистояти їм у межах, за яких наступає її руйнування

Боротьба зі злочинністю - сукупність мер економічного, політичного, правового, психологічного, організаційного, технічного характеру, спрямованих на ліквідацію, або ослаблення факторів, що сприяють здійсненню злочинів, на попередження, припинення, реєстрацію, розкриття й розшук злочинців, розслідування злочинів, на здійснення карного правосуддя, виправлення осіб, що зробили злочин, і контроль за їхнім

поводженням після відбування покарання, а також на відшкодування негативних наслідків злочинів.

Бюрократичні дії службовців державного й господарського апарата, що систематично вимагає хабарі за виконання посадових обов'язків по обслуговуванню клієнтури інших господарюючих суб'єктів.

Виктимність – це властивість однієї людини, (або певної соціальної групи), що виражається в схильності бути жертвою злочину.

Вірус комп'ютерний - невелика, досить складна, ретельно складена й небезпечна програма, що може самостійно розмножуватися, переносити себе на диски, прикріплюватися до чужих програм і передаватися по інформаційних мережах.

Впровадження спеціальних технічних засобів -незаконна, негласна установка спеціальних технічних засобів на об'єктах охорони. Виробляється в ході промислового шпигунства й несумлінної конкуренції.

"Злодій у законі": **1)**. Звання, що привласнює на спеціальній злодійській сходці особі, що володіє в середовищі професійних злочинців авторитетом, заснованим на значному злочинному досвіді, виявлених здатностях організовувати злочинні групи або керувати ними, дотриманні традицій і правил даного середовища або на внесенні великих сум у грошовий фонд злочинного співтовариства. **2).** Особа, що має відповідне звання й виконує функції: прийняття в складі "сообщаковій братви" (групи "злодіїв у законі" або авторитетів злочинного середовища) або самостійно - рішень по визначенню основних напрямків і форм злочинної діяльності, форм, джерел й обсягів поповнення грошових фондів злочинного співтовариства; взаємодії з організаторами й керівниками інших злочинних груп; "правосуддя" відносно членів злочинного співтовариства й деякі інші.

Вивідування – один із способів одержання інформації не гласно, що полягає в тім, що співробітник або агент спецслужби або правоохоронного органа, розмовляючи з інформованою

людиною, непомітно для останнього спонукує його розповісти про такі факти, події й відомості, які цікавлять ініціаторів завдання.

Вимагання - вимога передачі чужого майна або права на майно або здійснення інших дій майнового характеру під погрозою застосування насильства або знищення або ушкодження чужого майна, а дорівнює під погрозою поширення відомостей, що ганьблять потерпілого або його близьких, або інших відомостей, які можуть заподіяти істотна шкода правам або законним інтересам потерпілого або його близьких.

Газова зброя - зброя, призначена для тимчасової поразки живої мети за допомогою застосування сльозоточивих або дратівних речовин.

Грабіж - відкрите викрадення чужого майна, зроблене із застосуванням насильства, не небезпечного для життя або здоров'я, або з погрозою застосування такого насильства.

Диверсія - здійснення вибуху, підпалу або інших дій, спрямованих на руйнування або ушкодження підприємств, споруджень, шляхів і засобів повідомлення, засобів зв'язку, об'єктів життєзабезпечення населення з метою підриву економічної безпеки й обороноздатності.

Добування інформації - дії по зборі, аналізу, поширенню або зберіганню інформації, не призначеної для переказу гласності без згоди тих осіб, організацій і країн, яким дана інформація належить.

"Жучок" - радіомікрофон, установлений у приміщенні, технічних засобах, побутовій техніці різного призначення з метою перехоплення розмови.

Захоплення заручника – захоплення, або втримання особи як заручник, зроблені з метою спонуки держави, організації або громадянина зробити яка-небудь дія або втриматися від здійснення якої-небудь дії як умови звільнення заручника.

Захист інформації: **1)**. Система адміністративних мір і прийомів, спрямованих на класифікацію, контролювання й захист від несанкціонованого розголошення грифованої інформації

відповідно до законодавства. **2.)** Сукупність заходів, що забезпечують попередження несанкціонованого доступу до конфіденційної інформації, охоронюваним відомостям промислового, економічного, торговельного, фінансового й технічного характеру. **3.)** Охорона будь-якої інформації, кореспонденції, ідей, які надруковані, написані, висловлені усно окремою особою, організацією або урядом.

Зона надзвичайної ситуація - територія, на якій зложилася надзвичайна ситуація.

Джерело інформації - особа, предмет або вид діяльності, за допомогою яких добувається інформація.

Джерело конфіденційної інформації - носій інформації, за допомогою якого приватні детективи й охоронці одержують неофіційні відомості в ході розшукної або охоронної діяльності. Джерелом конфіденційної інформації можуть бути: фізичні і юридичні особи, документи, публікації в засобах масової інформації, об'єкти візуального спостереження й ін.

Інформаційна система - із сукупність фахівців, інформаційних ресурсів, технологій, що здійснює інформаційні процеси.

Інформаційні процеси - процеси збору, обробки, нагромадження, зберігання, актуалізації, поширення інформації.

Інформаційні ресурси - документи й масиви документів (бібліотеки, архіви, фонди, бази даних, бази відомостей), інші форми організації інформації із всіх напрямків життєдіяльності суспільства.

Інформації - це відомості, знання, повідомлення, які містять елементи новизни для їхнього одержувача й використаються в процесі ухвалення рішення.

Канал проникнення - фізичний шлях від зловмисника до джерела конфіденційної інформації, за допомогою якого можливий несанкціонований доступ до охоронюваних відомостей.

Якість інформації - ступінь практичної придатності інформації, використовуваної в процесі керування, обумовлена сукупністю таких властивостей, як повнота, щільність, корисність, вірогідність, цінність інформації.

Клептоманія - пристрасть до крадіжок.

Конкуренція - суперництво, змагання між виступаючими на ринку підприємцями, що мають метою забезпечити кращі можливості збуту своєї продукції, задовольняючи різноманітні потреби покупців

Консалтинг – це діяльність по консультуванню виробників, продавців і покупців по широкому колу економічних й інших питань, пов'язаних з господарством і вдачею

Конфліктна ситуація - гостра форма прояву протиріч. Виражається в зіткненні протилежних інтересів людей при спільній діяльності через розбіжність мотивів, цілей і способів їхнього рішення. Частота й складність конфліктної ситуації багато в чому залежить від ефективності матеріального стимулювання, рівня організації праці, виховної роботи, соціально-психологічного клімату в трудовому колективі, авторитету керівників і стилю керівництва.

Концепція захисту інформація - система поглядів, вимог й умов організації захисту охоронюваних відомостей від розголошення, витоку й несанкціонованого доступу до них через різні канали.

Концепція національної безпеки - система науково обґрунтованих й офіційно прийнятих поглядів на шляхи, засоби й механізми захисту від зовнішніх і внутрішніх погроз життєво важливим інтересам держави, територіальній цілісності й політичній стабільності, можливості стійкого соціально-економічного розвитку.

Корупція: 1). Використання особами, уповноваженими на виконання державних функцій, свого статусу й пов'язаних з ним можливостей для протиправного одержання матеріальних й інших благ і переваг, а дорівнює надання їм таких благ і переваг

фізичними і юридичними особами. **2).** Зрощування злочинного миру з державно-владними й виконавчими структурами держави.

Крадіжка - таємне розкрадання чужого майна.

Криміногенна обстановка - сукупність факторів, що сприяють збереженню або росту злочинності (окремих її пологів і видів) на певній території.

Крекер - різновид хэкеров, що займається злодійством чужої інформації.

Патентна злочинність - сума кримінально злочинних діянь, які не стають відомими державним правоохоронним органам протягом певного періоду часу на певній території й тому не відбиті в офіційній карній статистиці.

Легалізація - (відмивання) коштів або іншого майна, придбаного незаконним шляхом, здійснення фінансових операцій й інших угод з коштами або іншим майном, придбаним свідомо незаконним шляхом, а дорівнює використання зазначених засобів або іншого майна для здійснення підприємницької або іншої економічної діяльності.

Лжебанкрутство - свідомо помилкове оголошення юридичною особою про нездатність платити по своїх боргових зобов'язаннях, що переслідує, мету приховання викрадених, розтрачених сум.

Лжепідприємство - створення комерційних організацій без наміру здійснювати підприємницьку або банківську діяльність, що має метою одержання кредитів, звільнення від податків, витяг іншої майнової вигоди або прикриття забороненої діяльності, що заподіяло великий збиток громадянам, організаціям або державі.

Ліцензіат - фізична або юридична особа, що має ліцензію на здійснення конкретного виду діяльності.

Ліцензія - (дозвіл) документ, що надає право власникові на здійснення певного виду діяльності протягом установленого в ньому строку при обов'язковому дотриманні ліцензійних вимог.

Маргінальні явища - це негативні соціальні явища, (злочинних правопорушень,) зокрема пияцтво, наркоманія, токсикоманія, проституція.

Могутність держави - термін, що включає в себе десять основних показників розвитку держави: людський потенціал; територія й природні ресурси; військова сила; морально-політична єдність; національне багатство; рівень Науково-технічного розвитку; частка участі в міжнародному подолу праці, культурна спадщина й досягнутий рівень культури, рівень демократії й особистих воль, якість життя населення.

Моніторинг - процес відстеження стану системи або явища.

Морально-психологічний клімат - стан колективу, у якому виражаються особливості взаємодії й настрою працівників, ступінь їхнього задоволення змістом й умовами праці, стилем керування й інших факторів. Морально-психологічний клімат характеризується рівнем злагодженості й керованості, освоєнням нововведень, товариською взаємодопомогою, відсутністю або наявністю конфліктних ситуацій.

Шахрайство - розкрадання чужого майна або придбання права на чуже майно шляхом обману або зловживання довірою.

Незаконна банківська діяльність - здійснення банківської діяльності (банківських операцій) без реєстрації або без спеціального дозволу (ліцензії) у випадках, коли такий дозвіл (ліцензія) обов'язково, або з порушенням умов ліцензування, якщо це діяння завдало великої шкоди громадянам, організаціям або державі або сполучено з витягом доходу у великому розмірі.

Незаконне одержання кредиту - одержання індивідуальним підприємцем або керівником організації кредиту або пільгових умов кредитування шляхом надання банку або іншому кредиторові свідомо неправдивих відомість про господарське положення або фінансовий стан індивідуального підприємця або організації, якщо це діяння завдало великої шкоди.

Незаконне підприємництво - здійснення підприємницької діяльності без реєстрації або без спеціального дозволу (ліцензії) у випадках, коли таке рішення не приймалося.

Носії комерційної таємниці - люди, а також електронні поля й матеріальні об'єкти, у яких інформація знаходить своє відбиття: документи, записи, звіти, протоколи, креслення, матеріали, зразки, моделі, прилади, речовини й т.д.

"Ноу-хау": **1.)** Сукупність різних знань наукового, технічного, виробничого, фінансового, комерційного або іншого характеру, досвіду, практично застосовуваних у діяльності підприємства або в професійній діяльності, які ще не стали загальним надбанням. **2.)** Технічні знання, досвід, секрети виробництва, необхідні для рішення якого-небудь завдання. 3.) Повністю або частково конфіденційні знання, що включають відомості технічного, економічного, адміністративного, фінансового характеру, використання яких забезпечує перевага особі, їх що получили.

Суспільна безпека – це складений елемент національної безпеки, що включає в себе: систему захисту суспільства, людини від злочинності, корупції, тіньової економіки, будь-яких форм антисоціального поводження; скоординовану діяльність різних соціальних об'єктів по запобіганню можливих негативних соціальних наслідків переходу країни до ринкової економіки (ріст безробіття, збільшення розриву в рівні життя різних соціальних шарів суспільства, погіршення положення незаможних груп населення); комплекс мер по запобіганню соціальної напруженості в суспільстві у зв'язку з міжнаціональними, територіальними, політичними, економічними, конфесіональними й іншими конфліктами.

Організація захисту комерційної таємниці - реєстрація права на комерційну таємницю в уставі підприємства; визначення переліку посадових осіб, уповноважених класифікувати інформацію як комерційну таємницю; розробка внутрішніх правил засекречування, забезпечення схоронності комерційної таємниці й розсекречення утримуючих її відомостей; введення відповідного маркування документів й інших носіїв інформації й налагодження

секретного діловодства; установлення й підтримка режиму таємності, здійснення контролю за дотриманням режиму таємності.

Організована злочинність: 1.) Сукупність зареєстрованих протягом певного періоду на певній території злочинів, зроблених організованими групами. **2.)** Сукупність організованих злочинних груп й їхніх учасників, зареєстрованих протягом певного періоду на певній території. **3.)** Створення організованих груп, злочинних організацій, злочинних співтовариств й їхня злочинна діяльність.

Охорона - комплекс організаційних і технічних заходів щодо обмеження доступу й захисту території, приміщень, інформації, засобів і предметів виробництва, виробленої продукції.

Охорона об'єкта - здійснювані адміністрацією підприємства, фірми, банку й/або уповноваженим на те приватним охоронним підприємством заходу, спрямовані на попередження несанкціонованого доступу (проникнення) на охоронюваний об'єкт сторонніх осіб, а також заподіяння можливого матеріального збитку.

Охоронні заходи - сукупність дій по забезпеченню безпеки охоронюваних об'єктів і громадян.

Охоронювані об'єкти - будинку, будови, спорудження, транспортні засоби, інше майно, а також території, що підлягають захисту від протиправних дій.

Першочергові інформаційні потреби – це потреби затверджені компетентною особою або органом перелік найбільш важливих проблем, які представляють особливо великий інтерес для осіб, що приймають рішення в конкретній області діяльності.

Платоспроможність - здатність і можливість фізичної або юридичної особи вчасно й у повному розмірі оплатити свої борги. Платоспроможність є необхідною умовою для визнання даної особи кредитоспроможним, тобто заслуховує довіри для одержання кредиту.

Підробка документів - виготовлення повністю фіктивного документа (лист, авізо, вексель) або незаконна зміна справжнього документа; виправлення, заміна або знищення частини тексту,

внесення додаткових даних, відтворення підпису за іншу особу та інше.

Пожежна безпека об'єкта - комплекс заходів, спрямованих на приведення об'єкта в стан, при якому виключається можливість пожежі, а у випадку виникнення - забезпечення запобігання впливу на людей небезпечних факторів пожежі, забезпечення захисту матеріальних цінностей й їхньої схоронності.

Положення про службу безпеки - нормативно-правовий документ, що визначає склад, структуру й функціональні обов'язки підрозділів і співробітників служби безпеки.

Перевищення повноважень - діяння, зроблена керівником або службовцем приватної охоронної служби всупереч завданням своєї діяльності із застосуванням насильства або з погрозою його застосування.

Злочинне співтовариство – (злочинна організація), що має стійкі протиправні зв'язки з особами, уповноваженими на виконання державних або суспільних або інших привселюдно значимих функцій, для використання державних, суспільних структур, кредитно-фінансових установ, а також засобів масової інформації з метою одержання злочинних доходів.

Промислова таємниця - секрети виробничої діяльності підприємства, методи й способи керування фінансами, маркетингом, виробництвом, фінансами, виявлення яких конкуруючими фірмами може завдати істотної шкоди підприємству або розорити його.

Професійна етика - кодекс поводження, що забезпечує моральний характер тих взаємин між людьми, які випливають із їхньої професійної діяльності.

Радіозакладка - мініатюрний електронний пристрій, що складається з мікрофона, радіопередавача що забезпечує передачу переговорів, що підслухують, на значну відстань із допомогою електромагнітних хвиль. Радіозакладки комуфлюють під побутові й технічні прилади, складені елементи меблів, устаткування офісів і службових кабінетів.

Керівник організованої злочинної групи - учасник організованої злочинної групи, що володіє правом: віддавати вказівки, обов'язкові для виконання іншими учасниками групи; установлювати функції останніх усередині групи; визначати об'єкт (об'єкти) злочину (злочинів), час і способи його (їх) здійснення; розподіляти доходи від злочинної діяльності; приймати в групу й виключати із групи її учасників; вживати заходів по забезпеченню безпеки групи від карного переслідування.

Рекет - вимагання державного або особистого майна шляхом погроз і насильства.

Рекетир - злочинець, що займається рекетом, здирник, шантажист, гангстер.

Система захисту інформації - організована сукупність заходів, методів, органів і засобів, створюваних з метою захисту інформації.

Сфера впливу організованої злочинної груп - господарюючий суб'єкт (група господарюючих суб'єктів), територіальне утворення (район, населений пункт, регіон, група регіонів), галузь економіки або державна функція, керування й розвиток яких об'єктивно залежить або цілеспрямовано здійснюється з урахуванням інтересів злочинної групи.

Тіньова економіка - неконтрольоване суспільством виробництво, розподіл, обмін і споживання товарно-матеріальних цінностей, тобто приховувані від органів державного керування, громадськості соціально-економічні відносини між окремими громадянами, соціальними групами по використанню існуючих форм власності в корисливих особистих або групових інтересах.

Тероризм - здійснення вибуху, підпалу або інших дій, що створюють небезпеку загибелі людей, заподіяння значного майнового збитку або настання інших суспільно небезпечних наслідків, якщо ці дії зроблені з метою порушення суспільної безпеки, лякання населення або надання впливу на прийняття рішень органами влади, а також погроза здійснення зазначених дій у тих же цілях.

Технічний захист інформації - сукупність заходів і технічних засобів (механічних, оптичних, електричних й інших), що забезпечують захист інформації.

Технічні засоби контролю доступу - засоби систем контролю доступу на охоронювані території, у приміщення, сховища й інші простори і ємності.

Технічні засоби охорони - апаратні технічні засоби, що забезпечують контроль доступу, схоронність і протипожежну безпеку території, приміщень, сховищ й інших охоронюваних об'єктів.

Технологічний тероризм - застосування або погроза застосування терористами ядерної, хімічної, бактеріологічної зброї й інших радіоактивних речовин, а також спроба захоплення або виведення з ладу різного роду промислових й інших об'єктів (енергетики, хімії, зв'язку й т.д.), що мають важливе значення для економіки й/або представляє підвищену небезпеку для життя людей і навколишнього середовища.

Керування безпекою - система регулярних захисних заходів, спрямованих на забезпечення безпеки відповідно до зміни умов внутрішнього й зовнішнього середовища.

Рівень злочинності - число зроблених протягом певного періоду на певній території злочинів (осіб, їх що зробили) розраховуючи на 100 тис. (іноді на 10 тис.) людина, що досягли віку настання кримінальної відповідальності.

Витік інформації - неконтрольований вихід конфіденційної інформації за межі організації або кола осіб, якою ця інформація довірена.

Уразливість - властивість системи, що може привести до порушення її захисту при наявності погрози.

Фізична безпека - система зовнішніх і внутрішніх відносин підприємства, що забезпечує фізичну безпеку працівників підприємства, його клієнтів, фондів, матеріальних й інтелектуальних (інформаційних) цінностей від навмисного або

ненавмисного їхнього знищення, ушкодження їхніх якісних характеристик або розкрадання.

Фрек - телефонний хуліган, що за допомогою різних пристроїв і способів підключається до телефонних мереж, забезпечуючи безконтактне з'єднання незаконного абонента через лінії зв'язку.

Хекер - комп'ютерний хуліган, що незаконно підключається до чужих мереж.

Цінність інформації – властивість інформації, обумовлена її придатністю до практичного використання на основі обліку таких параметрів, як корисність, повнота, вірогідність, новизна.

Приватна детективна діяльність - надання на договірній основі детективних послуг на території України юридичними й (або) фізичними особами, зареєстрованими у встановленому порядку й що мають відповідні ліцензії, видані органами внутрішніх справ, з метою захисту законних прав й інтересів своїх клієнтів.

Приватна охоронна діяльність - надання на договірній основі охоронних послуг на території України юридичними особами, зареєстрованими у встановленому порядку й що мають відповідні ліцензії, видані органами внутрішніх справ, з метою захисту законних прав й інтересів своїх клієнтів.

Приватна детективна організація - організація, засновувана у формі господарського товариства або суспільства для надання детективних послуг.

Приватний охоронець - громадянин України, що одержав у встановленому Законом порядку ліцензію на приватну охоронну діяльність і працюючий у приватній охоронній організації або службі безпеки юридичної особи.

Приватна охоронна організація - організація, засновувана у формі господарського товариства або суспільства для надання охоронних послуг.

Використана література

1. Конституція України // Закони України.- Т.10.- К., 1997.
2. Закон України "Про інформацію" від 2.10.1992 р. // Закони України.- Т.4.- К., 1996.
3. Закон України "Про авторське право і суміжні права" від 23.12.1993 р. // Закони України.- Т.6.- К., 1996.
4. Закон України "Про державну таємницю" від 21.01.1994 р. // Закони України.- Т.7.- К., 1997.
5. Закон України "Про захист інформації в автоматизованих системах" від 5.07.1994 р. // Закони України.- Т.7.- К., 1997.
6. Закон України "Про підприємництво" від 7.02.1991 р. // Закони України.- Т.1.- К., 1996.
7. Закон України "Про підприємства в Україні" від 27.03.1991 р. // Закони Ук-раїни.- Т.1.- К., 1996.
8. Закон України "Про обмеження монополізму та недопускання недобросовісної конкуренції" від 18.02.1992 р. // Закони України.- Т.2.- К., 1996.
9. Закон України "Про захист від недобросовісної конкуренції" від 7.06.1996 р.- Т.10.- К., 1997.
10. Закон України "Про власність" від 24.04.1991 р. // Закони України.- Т.1.- К., 1996.
11. Постанова КМ України від 9 серпня 1993 р. №611 "Про перелік відомостей, що не становлять комерційної таємниці" // Збірник постанов Уряду України.- 1993.- №12
12. Тимчасове положення "Про охорону об'єктів промислової власності та раціоналізацію пропозицій в Україні", затверджено указом Президента від 18.09.1992 р.
13. Андрощук Д. Правове регулювання захисту від недобросовісної конкуренції // Україна: інформація і свобода слова.- К., 1997.
14. Апшер. Опасности "всемирной паутины" // Конфидент.- 1996.- №5.
15. Брягин О. Простая арифметика // Бизнес и безопасность.- 1998.- №1.- С.1-6.
16. Вехов В. Компьютерные преступления.- М., 1996.
17. Герасимов Б.М. Законопроект "О коммерческой тайне" - в стадии завершения // Вопросы защиты информации.- 1994.- №2.- С.50-52.
18. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы // Зарубежная радиоэлектроника.- 1993.- №3.- С.3-22.

19. Горячев В.С. Информация и ее защита // Вопросы защиты информации.- 1994.- №2.- С.38-45.

20. Григорьев М. Методы снятия информации в телефонных сетях // Сети.- 1997.- №3. -С.21-22.

21. Гудков В. Шпионы - там, шпионы - здесь. Можно ли подслушать переговоры в сети GSM? // Сети.- 1997.- №3.- С.20.

22. Дорошев В.В., Домарев В.В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно "Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)", США, "Оранжевая книга" // Бизнес и безопасность.- 1998.- №1.- С.19-21.

23. Задворний А. Інформаційна безпека і свобода слова в Україні // Україна: інформация і свобода слова.- К., 1997.

24. Иванов М.Н., Пахомова А.С. Подход к прогнозированию направлений промышленного шпионажа в отношении конкурентоспособних изделий // Вопросы защиты информации.- 1994.- №2.- С.31-33.

25. Крылов В. Информационные комьютерные преступления.- М., 1997.

26. Когут Ю.И. Безопасность фирмы // Безопасность информации.- 1996.- №3.

27. Кузнецов П.А. Информационная война и бизнес // Конфидент.- 1996.- №4.

28. Курило А.П. Об ответсвтенности за правонарушения при работе с информацией // Вопросы защиты информации.- 1994.- №2. -С.19-20.

29. Курило А.П., Стрельцов А.А. Проблемные вопросы обеспечения информационной безопасности в Российской Федерации // Вопросы защиты информа-ции.- 1994.- №2.- С.21-25.

30. Лаврентьев А.В. Организация в офисах защиты информации от утечки по техническим каналам // Безопасность информации.- 1996.- №3.

31. Мироненко. Правовые проблемы промышленной собственности // Действие законодательства Украины и практика его приминения: Реферативный обзор.- К., 1995.- С.52-65.

32. Мироненко. Правовые проблемы интелектуальной собственности // Действия законодательства Украины и практика его приминения: Реферативный обзор.- К., 1995.- С.65-77.

33. Полянский А., Белов В. Правовая охрана коммерческой тайны // Право и экономика.- 1994.- №3.

34. Степанов И. Шпиономания или обыкновенный промышленный шпионаж? // Бизнес и безопасность.-1997.- №5.- С.2-3, 21.

35. Цивільне право. Частина друга.- К.: Вентурі, 1996.

36. Гражданское право.- СПб, 1996.

37. Науково-практичний коментар Кримінального кодексу України.- К., 1997.

38. Кодекс Украины об административных правонарушениях.- Харьков, 1997.

39. Кримінальний кодекс України: Проект підготовлений робочою групою КМ України.- 1997.- С.138.

40. Белоусов А.И. Как защитить себя и свой бизнес. К-д. 2002.

41. Макмак В.П. Служба безопасности предприятия. Интернет издания . 2003.

Научно-популярное издание

В.Е.Карпов. П.Ф.Закревский

Менеджмент безопасности
(теория и практика)

2 том

(на украинском языке)

Рецензент: **Н.А.Свирень**, кандидат технических наук, профессор, академик.

Технический редактор: С. В. Лысенко

Компьютерная верстка: В. В. Безкровный

Печать: ЧП Лысенко С. В.

Здано в набор: 13.08.2007 г. Подп. к печати 21.09.2007 г.
Формат 60x84 1/16. Бумага офсетная. Печать офсентая.
Гарнитура Times New Roman CYR. Авт. лист. 16,0. Уч. изд. лист. 16,2
Тираж 1000.

340