ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Навчально-науковий інститут права, економіки та соціології

Кафедра правових основ підприємницької діяльності

заочна форма навчання

**КОНТРОЛЬНА РОБОТА**

**Тема: «Безпека підприємницької діяльності»**

м. Харків – 2010 р.

**План**

Вступ

1 Забезпечення охорони та режиму

2 Забезпечення захисту комерційної таємниці

3 Технічний захист

Висновок

Список використаної літератури

**Вступ**

В умовах ринкових відносин, коли держава вже не несе відповідальності за результати фінансово-господарської діяльності підприємства, забезпечення економічної безпеки стає однією з найбільш важливих і актуальних проблем його життєдіяльності.

Серед вітчизняних і зарубіжних учених-економістів немає єдиного визначення терміну „економічна безпека”. Разом з тим, принципових розходжень у підходах до трактування змісту даної економічної категорії не спостерігається.

Найбільш поширеним є визначення економічної безпеки підприємства як стану ефективного використання його ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і існуючих ринкових можливостей, що дозволяє запобігати внутрішнім і зовнішнім негативним впливам (загрозам) і забезпечити його тривале виживання і стійкий розвиток на ринку відповідно до обраної місії.

**1 Забезпечення охорони та режиму**

На всіх великих і середніх підприємствах (в організаціях) звичайно створюються автономні служби безпеки, а безпека функціонування невеликих фірм може забезпечуватися територіальними (районними або міськими) службами, що в них фірма наймає одного чи кількох охоронців.

Такі служби охорони, як правило, створюються при місцевих органах внутрішніх справ або при державній службі безпеки.

Служба безпеки будь-якої фірми постійно виконує певний комплекс завдань. Головними з них для будь-якої фірми є такі:

1) охорона виробничо-господарської діяльності та захист відомостей, що вважаються комерційною таємницею даної фірми (підприємства, організації);

2) організація роботи з правового та інженерно-технічного захисту комерційних таємниць фірми;

3) запобігання необґрунтованому допуску й доступу до відомостей та робіт, які становлять комерційну таємницю;

4) організація спеціального діловодства, яке унеможливлює несанкціоноване одержання відомостей, віднесених до комерційної таємниці відповідної фірми;

5) виявлення та локалізація можливих каналів витоку конфіденційної інформації в процесі звичайної діяльності та за екстремальних ситуацій;

6) організація режиму безпеки за здійснення всіх видів діяльності, включаючи зустрічі, переговори й наради в рамках ділового співробітництва фірми з іншими партнерами;

7) забезпечення охорони приміщень, устаткування, офісів, продукції та технічних засобів, необхідних для виробничої або іншої діяльності;

8) організація особистої безпеки керівництва та провідних менеджерів і спеціалістів фірми;

9) оцінка маркетингових ситуацій та неправомірних дій конкурентів і зловмисників.

Зрозуміло, що перелік конкретних завдань стосовно організації системи безпеки фірми залежно від специфіки її діяльності може бути більшим або меншим, але він завжди має бути достатнім та обґрунтованим.

**Функції, об'єкти та управління безпекою**. Сукупність конкретних завдань, що стоять перед службою безпеки фірми, зумовлює певний набір виконуваних нею функцій. Загальні функції, що покладаються на службу безпеки фірми (підприємства, організації).

• Організація і забезпечення пропускного та внутрішньо об’єктного режиму в приміщеннях; порядок несення служби; контроль дотримання вимог режиму персоналом фірми і партнерами (відвідувачами)

• Участь у розробці основоположних документів (статуту, правил внутрішнього розпорядку, договорів тощо) з метою відображення в них вимог організації безпеки й захисту (комерційної таємниці

• Розробка та здійснення заходів із забезпечення роботи з доку ментами, що містять відомості, які є комерційною таємницею, контроль виконання вимог матеріалів інструктивного характеру

• Виявлення і перекриття можливих каналів витоку конфіденційної інформації, облік та аналіз порушень режиму безпеки працівниками фірми, клієнтами та конкурентами

• Організація та проведення службових розслідувань за фактами розголошення або втрати документів, інших порушень безпеки фірми

• Розробка, оновлення і поповнення переліку відомостей, що становлять комерційну таємницю, та інших нормативних актів, які регламентують порядок організації безпеки й захисту інформації

• Забезпечення суворого виконання вимог нормативних документів з питань захисту комерційної таємниці

• Організація та регулярне проведення навчання працівників фірми й служби безпеки за всіма напрямками захисту комерційної таємниці

• Ведення обліку сейфів і металевих шаф, що в них дозволене постійне чи тимчасове зберігання конфіденційних документів, а також облік та охорона спеціальних приміщень і технічних засобів у них

• Підтримка контактів із правоохоронними органами та службами безпеки сусідніх підприємств (організацій) в інтересах вивчення криміногенної обстановки в районі (зоні)

У нормативних документах, які визначають організацію діяльності служб безпеки фірм, виокремлюються конкретні об'єкти, що підлягають захисту від потенційних загроз і протиправних посягань. Беручи загалом, до них належать:

• персонал (керівні працівники; персонал, який володіє інформацією, що становить комерційну таємницю фірми);

• матеріальні засоби праці та фінансові кошти (приміщення, споруди, устаткування, транспорт; валюта, коштовні речі, фінансові документи);

• засоби та системи комп'ютеризації діяльності фірми (підприємства, організації);

• технічні засоби та системи охорони й захисту матеріальних та інформаційних ресурсів.

Служба безпеки фірми завжди має бути готовою до подолання критичної (кризової) ситуації, що може постати через зіткнення інтересів бізнесу та злочинного світу. Для управління безпекою багато які фірми створюють так звані кризові групи, до складу яких входять керівник фірми, юрист, фінансист і керівник служби безпеки. Головна мета діяльності кризової групи — протидіяти зовнішнім загрозам для безпеки фірми

**2 Забезпечення захисту комерційної таємниці**

охорона безпека інформація таємниця

Умовно виділяють два види охорони інформації, що використовуються в підприємницькій діяльності, тобто два види інформаційної безпеки: пасивну й активну.

**Пасивна охорона** характеризується тим, що власник інформації надає їй режим відкритості, доступності для всіх зацікавлених осіб, але ці особи не можуть використовувати її в комерційних цілях. Саме власникові належить виключне право дозволяти кому-небудь використовувати цю інформацію. Таку охорону інформації встановлюють патентне та авторське право. Захист інтересів власника інформації у випадку її несанкціонованого використання реалізується в судовому порядку на підставі законодавства України.

Прикладів інформаційних об’єктів, на які їхні власники поширюють пасивну охорону, досить багато: винаходи, корисні моделі, промислові зразки (дизайн), товарні знаки, фірмові найменування, музичні, драматичні, аудіовізуальні, літературні, письмові здобутки різного характеру, комп’ютерні програми, лекції тощо.

**Активна охорона** інформації, що більше підходить для охорони комерційної таємниці від несанкціонованого власником використання, пов’язана з тим, що власник встановлює певний режим доступу, наприклад, обмежує доступ до інформації вузьким колом фахівців з числа персоналу, організує режимні зони на підприємстві, використовує носії інформації, що роблять неможливим несанкціоноване копіювання тощо.

Прикладом інформації, що може підпадати під активну охорону, та становити комерційну таємницю можуть служити відомості типу “ноу-хау”, тобто відомості технічного характеру – режими, методики, технологічні карти тощо, результати різних досліджень, методи управління, а також інформаційні об’єкти, що мають настільки значну комерційну цінність, що власник – з міркувань доцільності або безпеки – надає цій інформації режим обмеження доступу.

На сьогоднішній день втратам комерційної таємниці в Україні сприяє безсистемність її захисту. Спостерігається роз’єднаність зусиль держави і приватних підприємців у забезпеченні цілісності інформації, відсутність у власників комерційної таємниці організаційного досвіду щодо її захисту, недостатність правової підготовки та інформаційної культури.

При застосуванні організаційно-правового механізму захисту комерційної таємниці постає цілий ряд невирішених питань, серед яких відсутність чіткого визначення поняття “комерційна таємниця” з урахуванням інтересів як юридичних, так і фізичних осіб; розробки механізму здійснення прав власності на інформацію, віднесену до комерційної таємниці; методики визначення її вартості; визначення органу державної виконавчої влади, що буде формувати й реалізовувати державну політику щодо охорони прав на комерційну таємницю тощо.

Що стосується визначення органу державної виконавчої влади, який буде формувати й реалізовувати державну політику щодо охорони прав на комерційну таємницю, Законом України “Про Службу безпеки України” в статті 25 визначено, що до обов’язків СБУ віднесено “сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України”. Як бачимо, формулювання даної норми не дозволяє чітко визначити, чи є СБУ саме тим органом державної виконавчої влади, який буде формувати і реалізовувати державну політику щодо охорони прав на комерційну таємницю, чи ні. Крім того, законодавець не визначає, що розуміється під поняттям “сприяти”, а також механізм реалізації цього “сприяння”.

**3 Технічний захист**

Одним з найважливіших частин захисту інформації підприємства є технічний захист.

Витік інформації в комп'ютерних системах може бути допущений як випадково, так і навмисно, з використанням технічних засобів знімання інформації.

Засоби протидії випадкового витоку інформації, причиною якої може бути програмно-апаратний збій або людський фактор, можуть бути розділені на наступні основні функціональні групи: дублювання інформації, підвищення надійності комп'ютерних систем, створення відмовостійких комп'ютерних систем, оптимізація взаємодії людини і комп'ютерної системи, мінімізація збитків від аварій і стихійних лих (в тому числі, за рахунок створення розподілених комп'ютерних систем), блокування помилкових операцій користувачів.

Найбільший інтерес представляє навмисна зміна інформації, також відоме як промислове (технічний) шпигунство.

Під час захисту інформації в комп'ютерних системах (КС) від традиційного шпигунства і диверсій використовуються ті ж засоби і методи захисту, що і для захисту інших об'єктів, на яких не використовуються КС. Для захисту об'єктів КС від загроз даного класу повинні бути вирішені наступні завдання:

• створення системи охорони об'єкта;

• організація робіт з конфіденційними інформаційними ресурсами на об'єкті КС;

• протидія спостереження;

• протидія підслуховування;

• захист від злочинних дій персоналу.

Дослідження практики функціонування систем обробки даних і комп'ютерних мереж показали, що існує досить багато можливих напрямів витоку інформації та шляхів несанкціонованого доступу до неї в системах та мережах:

- перехоплення електронних випромінювань;

- примусово електромагнітне опромінення (підсвічування) ліній зв'язку;

- застосування "підслуховуючих" пристроїв;

- дистанційне фотографування;

- перехоплення акустичних хвильових випромінювань;

- розкрадання носіїв інформації і виробничих відходів систем обробки даних;

- зчитування інформації з масивів інших користувачів; o читання залишкової інформації в апаратних засобах;

- копіювання носіїв інформації і файлів з подоланням заходів захисту;

- модифікація програмного забезпечення шляхом виключення або додавання нових функцій;

- використання недоліків операційних систем і прикладних програмних засобів;

- незаконне підключення до апаратури та ліній зв'язку, в тому числі в якості активного ретранслятора;

- зловмисний вивід з ладу механізмів захисту;

- маскування під зареєстрованого користувача і присвоєння собі його повноважень;

- введення нових користувачів;

- впровадження комп'ютерних вірусів.

**Висновок**

Підсумовуючи все вищевказане, можна зробити висновок, що при рівні технологічного прогресу, який ми маємо на сьогодні є доволі багато факторів які можуть нанести матеріальну шкоду будь-якого підприємства. Саме тому служба безпеки повинна бути присутньою на кожному з них.

**Список використаної літератури**

1. Бабаш А.В.,Шанкин Г.П. История криптографии.Ч.1. - Гелиос АРВ, 2002. – 240с.

2. Бабаш А.В., Шанкин Г.П. Криптогорафия. – Москва: СОЛОН-Р, 2002, 511с.;

3. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.

4. Вехов. Компьютерные преступления, Москва: СОЛОН-Р 2006, c. 14.

5. Гмурман А.И. Информационная безопасность. М.: «БИТ-М», 2004 г.

6. Дъяченко С.И. Правовые аспекты работы в ЛВС. СП-б, «АСТ», 2002 г.

7. Диффи У., Хеллман М. Защищенность и имитостойкость. // ТИИЭР. – 1979. – Т.67, №3. – С.71-109.

8. Ермаков С.М. Метод Монте-Карло и смежные вопросы. - М.: Наука, 1975. - 472с.