УДК 347.7+334.722

Я. В. ГУДОВ

Міжрегіональна Академія управління персоналом, м. Київ

СИСТЕМА БЕЗПЕКИ ПІДПРИЄМСТВА

Наукові праці МАУП, 2009, вип. 1(20), с. 222–229

Розкрито сутність системи безпеки підприємства, поставлені завдання перед службою безпеки та визначено основні принципи її діяльності. Враховано кваліфікацію та знання в різних галузях керівника служби безпеки підприємства та його підлеглих. Акцентовано увагу на різних видах безпеки підприємства. Визначено можливі методи і засоби протиправних посягань на комерційне майно та інформацію, а також заходи щодо їх протидії та ліквідації; встановлено необхідні контакти із зовнішніми організаціями, що здатні сприяти забезпеченню захисту підприємства.

На теренах України можна займатися будь-якою підприємницькою діяльністю, що не заборонена законом. З одного боку, держава підтримує конкуренцію для забезпечення економічної різноманітності в суспільстві, з іншого — захищає конкуренцію у підприємницькій діяльності, не допускає цінової дискримінації та зловживань монопольним становищем на ринку.

В Україні визнається і діє принцип верховенства права. Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй. Норми Конституції України є нормами прямої дії. Звернення до суду для захисту конституційних прав і свобод людини і громадянина безпосередньо на підставі Конституції України гарантується [1, ст. 8].

Так, багаторівнева економіка потребує різноманітних видів забезпечення економічної, фізичної та інших видів безпеки, організації охорони. Виходячи з того, що збільшується частка приватного капіталу в економіці України, розвитку малого та середнього бізнесу, роздержавлення стратегічних державних об'єктів, підприємств базової сфери економіки, стає актуальним питання щодо організації комерційної безпеки на підприємствах.

Необхідно зрозуміти той факт, що саме з розвитком підприємницької діяльності в Україні в умовах конкурентного середовища набули негативних обертів такі явища, як підслуховування, викрадення конфіденційної інформації, зняття інформації з технічних каналів через комп'ютерні мережі. Важливою проблемою перед суб'єктами підприємницької діяльності стало вирішення такого питання, як інформаційна безпека підприємств. Варто визначити інформаційну безпеку як здатність персоналу підприємства забезпечити захист інформаційних ресурсів і потоків від загроз несанкціонованого доступу до них.

Варто наголосити на тому, що останнім часом розвиток суспільства характеризується негативною динамікою не тільки зловмисних порушень роботи інформаційних систем чи мереж, а й злочинів, вчинених з використанням новітніх технологій, найсучаснішої техніки.

Розвиток комп'ютерів і комунікаційних систем фундаментально змінив принципи, на яких будується діяльність комерційних структур. До того, як технології увійшли в наше життя, ми виходили з ряду передбачень й опиралися на те, що називається "соціальними механізмами" забезпечення безпеки. Ми виходили з того, що інформація із запечатаного конверта нікуди не дінеться, ми визнавали вірогідність будь-яких відомостей, якщо унизу аркуша паперу, на якому вони були написані, стояв підпис людини, яка повідомляла нам цю інформацію, і ми вважали, що зберігаємо конфіденційність, якщо обговорюємо "таємні" питання за закритими дверима.

У зв'язку з бурхливим розвитком локальних і глобальних обчислювальних мереж удосконалюються і методи розвідки (комерційного шпигунства), спрямовані на перехоплення інформації, що обробляється, передається, зберігається у локальних мережах [7].

Нині важко відповісти — розвідувальною діяльністю більше займаються на рівні держав чи комерційних фірм, підприємств — конкурентів.

Відповідно швидко вдосконалюються і методи протидії розвідці [14].

Не випадково останнім часом розвиваються методи перехоплення інформації за допомогою каналів побічного електромагнітного випромінювання і наведень (ПЕМВН) елементів локальної мережі ПК [12].

Однак з того часу, як у нашому житті з'явилися комп'ютери, які ми використовуємо у бізнесі, такі припущення руйнуються, і наслідки можуть виявитися страшними. Більше того, до шахрайства можуть вдаватися тепер люди, які використовують системи здійснення угод, видаючи себе за законних користувачів і одержуючи в результаті цього доступ до конфіденційної інформації; аналогічно в діалоговий режим можуть втручатися хакери, які пробиваються через всі захисні редути. Так, якщо двоє людей спілкуються за допомогою електронної пошти, вони не бачать один одного, і не зрозуміло, як кожний з них може ідентифікувати іншого. Далі, якщо не використовувати спеціальних засобів захисту, будь-який користувач, що має в комп'ютері якусь важливу інформацію, не може надійно контролювати доступ до неї.

Більшість користувачів комп'ютерів мають на своїх столах "персоналки", і значна їх частина об'єднані між собою мережами. Творці такого способу переконують, що він різко збільшує комунікаційні можливості користувачів і швидкість доступу до потрібної інформації. За останній час вказана цифра не стала вищою. На жаль, надані вигоди часто супроводжуються проблемами у сфері забезпечення безпеки. У зв'язку з цим перед керівництвом завжди стоїть дилема, як забезпечити баланс переваг, наданих вільним доступом до інформації, і ризиків, які це супроводжують, і тільки прийнявши для себе рішення, що стосується загальних підходів, можна визначити, скільки потрібно коштів на забезпечення безпеки в нових умовах.

Тому, враховуючи сучасні наукові тенденції, положення загальної теорії системи, служба безпеки конкретного підприємства, виходячи із системного представлення про роботу по забезпеченню безпеки, розробляє свою концепцію оптимальних заходів щодо захисту робітників комерційної таємниці та майна. Це розглядається з точки зору практики як протидія на неправові методи отримання інформації (економічної, науково-технічної) іншими суб'єктами підприємництва. Системний підхід дає змогу приділити увагу побудові єдиного цілого на відміну від побудови компонентів чи підсистем. Отже, система являє собою не тільки єдність її складових, а дещо більше: організовану єдність у рамках цілого [3, *5*].

Втрата будь-якого елемента, підсистеми, його ослаблення несуть загрозу для всієї системи, можуть завдати шкоду будь-якого характеру. Мають місце деструктивні наслідки.

Відштовхуючись від цього поняття, можна визначити систему безпеки підприємництва як сукупність елементів, підсистем, що мають на меті виявлення, попередження, зниження, послаблення, нейтралізацію, припинення, локалізацію, відображення, усунення загроз.

Під безпекою варто розуміти стан об'єкта підприємства у системі його зв'язків з погляду здатності до стійкості (самовиживання) і розвитку в умовах внутрішніх і зовнішніх загроз до важко прогнозованих негативних факторів [10, *49*].

Однією з найважливіших складових економічної безпеки є безпека фінансова. Саме під фінансовою безпекою варто розуміти наступне:

1) рівень забезпечення громадянина, домашнього господарства, населення, підприємства, організації, установи, регіону, галузі, сектора економіки, ринку, держави, суспільства, державних утворень, світового співтовариства фінансовими ресурсами, достатніми для задоволення їх потреб;

2) стан фінансової, грошово-кредитної, валютної, банківської, бюджетної, податкової, інвестиційної систем, який характеризується збалансованістю, стійкістю до внутрішніх і зовнішніх негативних впливів, здатністю забезпечити ефективне функціонування національної економічної системи та економічне зростання.

Систему елементів фінансової безпеки складають:

1. Теорія фінансової безпеки.
2. Концепція фінансової безпеки.
3. Політика фінансової безпеки.
4. Стратегія і тактика забезпечення фінансової безпеки.
5. Структурні підрозділи фірми, що забезпечують фінансову безпеку.
6. Індикатори фінансової безпеки.
7. Інформація про фактичний стан фінансової безпеки.

Концепція фінансової безпеки має містити пріоритетні цілі та завдання забезпечення безпеки, шляхи та методи їх досягнення. Послідовність розроблення та реалізації концепції фінансової безпеки виглядає таким чином:

- розроблення законодавчої бази у сфері фінансової безпеки на рівні фірми;

- формування концепції фінансової безпеки комерційної структури;
- розроблення стратегії фінансової безпеки фірми;
- розроблення і реалізація тактичних заходів у сфері фінансової безпеки;
- контроль за виконанням визначених завдань і внесення необхідних коригувань.

Створення дійової системи фінансової безпеки передбачає чітке визначення джерел потенційної загрози у тій чи іншій сфері, а також наявних і необхідних ресурсів для їх нейтралізації. Причому загроза може бути наслідком як непередбачених обставин, випадкових подій, так і усвідомлених провокацій, злочинів усіх видів [11, *109–111*].

Побудова системи безпеки підприємства вимагає реалізації наступних завдань:

1) виявлення загроз для стабілізації і розвитку підприємства і вироблення заходів для їх протидії;

2) забезпечення захисту технологічних процесів;

3) реалізація мір протидії для всіх видів шпигунства (промислового, науково-технічного, економічного та ін.); під "підприємницьким шпигунством" варто розуміти систему методів, прийомів і засобів збирання відомостей про підприємство, виробництво, його діяльність. Так, Закон України "Про захист від недобросовісної конкуренції" від 7 червня 1996 р. [2] розкриває основні ключові поняття системи заходів щодо захисту безпеки підприємництва. Підприємницьке шпигунство має на меті досягнення конкуренції будь-якими заходами, зміцнення своїх економічних позицій, завдання шкоди тому, чия комерційна таємниця була використана. Такі відомості можуть бути отримані не тільки в результаті активних таємних заходів, а й шляхом збирання, систематизації та дослідження інформації, добутої з відкритих джерел (наприклад, веб-сайти та ін.);

4) своєчасне інформування керівництва про факти порушення законодавства з боку державних і муніципальних органів, комерційних і некомерційних організацій, що торкаються інтересів підприємства;

5) попередження переманювання співробітників підприємства, що володіють конфіденційною інформацією;

6) всебічне вивчення ділових партнерів, конкурентів, клієнтів;

7) своєчасне виявлення та адекватне інформування щодо дезінформуючих заходів;

8) формування через ЗМІ позитивної думки у клієнтів про економічний стан діяльності об'єкта;

9) захист законних інтересів підприємства та його співробітників;

10) збирання, аналіз, оцінювання і прогнозування даних, що характеризують обстановку на підприємстві;

11) своєчасне виявлення злочинних намагань, спрямованих на виявлення у персоналу підприємства секретів;

12) попередження проникнення на підприємство громадян, що порушують громадський порядок, та осіб — членів організованих злочинних груп;

13) своєчасне виявлення конфліктних ситуацій серед персоналу підприємства, розвитку деструктивних тенденцій, вирішення виникаючих проблем у трудовому колективі;

14) розроблення і вдосконалення локальних (корпоративних) норм, спрямованих на забезпечення безпеки підприємства;

15) розроблення заходів щодо захисту комерційної та іншої інформації;

16) розроблення заходів щодо протидії недобросовісної конкуренції;

17) організація взаємодії з правоохоронними і контролюючими органами з метою попередження і припинення правопорушень, спрямованих проти інтересів підприємства;

18) реалізація заходів щодо загроз фізичної безпеки (попередження).

Цей перелік завдань не є вичерпним. Кожна служба безпеки підприємства реалізує ті завдання, що стосуються мети створення підприємства чи його діяльності, тобто може скорочуватися чи збільшуватися залежно від специфіки діяльності фірми.

Тому система безпеки підприємства побудована на основі таких принципів:

1) централізованого управління;

2) координація та взаємодія з правоохоронними органами;

3) відповідності внутрішнім і зовнішнім загрозам;

4) пріоритетності заходів попередження;

5) законності заходів безпеки, тобто вони розробляються на основі і в рамках діючих нормативно-правових актів;

6) ієрархічності;

7) корпоративні правові акти підприємства не повинні суперечити законам і підзаконним правовим актам;

8) комплексного використання сил і засобів.

Варто наголосити на тому, що важливу роль у системі забезпечення безпеки підприємства відіграють співробітники служби безпеки. Так, працівників служби безпеки можна поділити на кілька категорій: охоронці (займаються фізичною охороною об'єктів підприємства), персональні охоронці або бодіґардс (до їхньої компетенції входить захист керівників підприємства та їх структурних підрозділів), спеціалісти (техніки, психологи, оперативники). Вимоги до різних категорій різні, враховуючи специфіку діяльності. На сьогодні спеціалісти повинні мати знання в таких галузях: інформаційно-аналітична робота, методи розвідки і контррозвідки, оперативна робота, соціальна психологія і психологія особистості, основи банківської справи і бухгалтерський облік, основи менеджменту та маркетингу, цивільне та кримінальне право.

Таким чином, грамотний спеціаліст зобов'язаний: вміти розробляти комплексні заходи щодо забезпечення безпеки комерційної фірми та особистої безпеки її керівництва; здійснювати захист комерційної інформації, у тому числі такої, що зберігається в комп'ютерних мережах; вміти застосовувати технічні засоби прихованого спостереження та прослуховування; вміти протидіяти проведенню подібних заходів конкурентами; розумітися на фінансовій звітності; займатися профілактикою правопорушень всередині фірми; проводити внутрішнє розслідування випадків крадіжок, шахрайства, саботажу та фінансових злочинів; організовувати перевірки (у тому числі негласні) порядності співробітників фірми; виявляти випадки співпраці співробітників фірми з конкурентами чи кримінальними структурами; співробітничати з правоохоронними органами під час розслідування злочинів, що вчиняються на фірмі; вміти готувати документи, які містять аналіз фінансово-економічного становища партнерів, оцінку конкурентів і потенційних клієнтів; вирішувати внутрішні конфлікти на фірмі; користуватися методикою виявлення в товарно-супроводжувальних документах (коносаментах, накладних), документах митних, фінансових, податкових органів ознак шахрайства чи злочинної діяльності, спрямованої проти фірми; користуватися методикою виявлення фальсифікації експортних товарів; розпізнавати ознаки та методи виявлення шахрайства, незаконних махінацій щодо відмивання коштів, здобутих злочинним шляхом; застосовувати методику виявлення махінацій з торговою маркою, вагою, об'єктом, технічними характеристиками продукції (особливо імпортної), елементів її виготовлення з порушенням техніки безпеки; виявляти недобросовісну рекламу з боку вітчизняних і зарубіжних фірм, випадки маніпуляцій, що здійснюються іноземцями з підставними компаніями чи особами [11, *265*].

Отже, виконання поставлених завдань вимагає не тільки "фізичної" безпеки підприємства, а й захисту інформації. Адже на сучасному етапі технічний розвиток призвів до появи все нових зразків складної за своєю будовою спецтехніки, що дає можливість заволодіти таємною інформацією підприємства, перебуваючи поза підприємством: за допомогою комп'ютера, інтернет-мережі, внутрішніх каналів зв'язку (локальні). Інформація підприємства знаходиться, як правило, на серверах. Обмін, передання інформації здійснюється всередині підприємства локальною мережею. Для більшої безпеки визначається, яка інформація є більш секретною, створюються відповідні рівні для її захисту, обмежується коло працівників з доступом до цієї інформації. Також розробляється ймовірний портрет злочинця: враховується його кваліфікація, спецтехніка та ін. Загрози електронної інформації на робочому комп'ютері поділяються на зовнішні і внутрішні.

Зовнішні загрози можуть створювати клієнти, консультанти, контролери, партнери, аудитори, керівники та службовці фірм, які займаються шпигунством, злочинні угруповання.

До внутрішніх загроз належать: перехоплення випромінювання монітора, що передається в комп'ютерних мережах і каналах зв'язку; фізичне або логічне пошкодження апаратно-програмних засобів або інформаційних архівів; комп'ютерні віруси; крадіжки апаратно-програмних засобів та інформаційного програмування; незаконне програмування продуктів, документів; мікрофонний ефект та ін.

Основними засобами захисту є екранування металевого корпусу монітору та системного блоку, а також використання пристроїв, що маскують побічне електромагнітне випромінювання; специфічне розташування моніторів, на яких обробляється інформація з обмеженим доступом.

Найвідоміші сьогодні перехоплення — це випромінювання моніторів. Монітор є "найголоснішим" випромінюючим елементом, оскільки для нормальної роботи електронно-променевої трубки необхідні високі рівні сигналів. Для дешифрування перехоплених сигналів монітора не потрібно складного опрацювання. Зображення на екрані монітора, випромінювані ним сигнали

багаторазово повторюються. У професійній апаратурі ця обставина використовується для накопичення сигналів та ефективнішої діяльності розвідки.

Професійна апаратура для перехоплення випромінювання монітора і відображення інформації коштує десятки тисяч доларів. Якщо розвідувальна апаратура встановлена на невеликій відстані, наприклад у сусідній квартирі, то для перехоплення випромінювання монітора може використовуватися саморобна апаратура, найдорожчим елементом якої є монітор комп'ютера, або навіть дещо доопрацьований побутовий телевізор.

Перехоплення інформації за рахунок випромінювання принтерів, клавіатури потребує менших витрат. Інформація у цих пристроях перехоплюється послідовним кодом, усі параметри якого стандартизовані й широко відомі.

Адміністратори локальної комп'ютерної мережі застосовують усі можливі засоби для розмежування доступу, входять у мережу лише з визначеної станції, коли нікого немає. Однак їм необхідно пам'ятати про радіовипромінювання, а непоганий малогабаритний професійний розвідувальний приймач нині коштує лише кілька сотень доларів.

Інформація, що передається в ефір за рахунок випромінювання принтерів і клавіатури, — це фактично метод радіорозвідки з використанням прихованого випромінювання.

Персональний комп'ютер є центральною ланкою в системі автоматизованої обробки інформації, тому він привертає особливу увагу конкурентів, правопорушників і розвідувальних служб [8].

Комп'ютер може випромінювати в ефір не лише ту інформацію, що опрацьовує. Якщо при його збиранні не було вжито спеціальних заходів, то він може слугувати також і джерелом відтоку мовної інформації. Це так званий "мікрофонний ефект", він може здійснюватися навіть через корпус комп'ютера. Під впливом акустичних коливань у корпусі змінюються розміри щілин та інших елементів, через які здійснюється випромінювання. Відповідно випромінювання стає модульованим, і все, що ви говорите біля комп'ютера, можна прослухати за допомогою розвідувального приймача. Якщо ж до комп'ютера підключені звукові колонки, то шпигун взагалі може заощадити на встановленні у приміщенні, що прослуховується, "жучків".

"Жучок" — це радіомікрофон, встановлений у приміщенні, вмонтований у побутову техніку різного призначення, з метою фіксації аудіоінформації [11, *309*].

Таким чином, щоб уникнути відтоку інформації через канали паразитного випромінювання, необхідно захищатися [6].

Багатоплановий підхід до інформаційних ресурсів зумовлює необхідність враховувати такий суттєвий фактор, як функціонування підприємства за умов ринкових відносин, характерною прикметою яких є боротьба між незалежними суб'єктами господарювання на ринку і гостра конкуренція товаровиробників. Боротьба за економічне виживання — закон ринку [4].

Багаторічна практика отримання доступу до економічних і промислових секретів конкурентів і конфіденційних відомостей комерційного характеру неодноразово засвідчувала, що це є ефективним засобом користування достовірною інформацією в усіх галузях ринкової економіки [13].

Методи проникнення у комп'ютерну мережу з метою наступного викрадення інформації різноманітні, найдійовіший — це встановлення в системі програми-закладки.

Програма-закладка, залежно від поставленої мети, може, наприклад, перехоплювати паролі користувачів або за визначеним критерієм знаходити необхідну інформацію на жорстких дисках. Усі системні адміністратори вживають відповідних заходів з попередження спроб відправити електронною поштою зібрану правопорушником інформацію на завчасно обумовлену адресу. Це змушує порушників вигадувати нові методи проникнення до комп'ютерної мережі.

Відтік або втрата конфіденційної інформації та вихід з ладу обладнання може статися внаслідок не зумисних помилок користувача; умисних шкідливих дій користувача; таємного введення в систему програм-закладок з вірусами "троянський кінь", "черв'як" та ін.

На заваді розвідувальної діяльності стоять великі обсяги програми-закладки та даних, що передаються за її допомогою.

Саме збирання відомостей дає змогу на основі застосування науково-розробленої системи методів пояснити суть виявлених процесів, пов'язаних з економічним становищем конкурента, виробити реакцію на вплив ситуації, подумки сформувати прогностичну модель найоптимальніших способів дій і межі поведінки в процесі використання інформації [5].

Скільки існує людство, стільки існує й проблема обміну інформацією. З одного боку, люди праг-

нуть спілкуватися та обмінюватися інформацією, а з іншого — намагаються приховати від сторонніх як зміст, так і факт її передання. Тому людство постійно вдосконалює засоби перехоплення і приховування. Для приховування інформації застосовують методи криптографії і стеганографії.

Криптографія — це система зміни інформації, щоб вона була зрозумілою лише для посвячених.

Стеганографія — це система зміни інформації з метою приховування самого факту існування таємного повідомлення. Слово "стеганографія" походить від слів "steganos" — таємниця і "graphy" — запис і буквально означає "таємний запис". Застосування криптографії дає змогу сторонньому спостерігачеві легко встановити факт передання таємного повідомлення, а стеганографії — приховувати це, більше того, для підвищення рівня захисту таємна інформація може додатково шифруватися.

Методи стеганографії передбачають, що сам факт будь-якого обміну інформацією не приховується, хоча повідомлення обов'язково переглядає цензор. Тому під приховуванням факту існування таємного повідомлення розуміється не лише (можливо, навіть не стільки) те, що цензор не може виявити у повідомленні, яке переглядається, іншого, прихованого повідомлення, а й те, що переказуване повідомлення не повинно викликати у цензора підозри. Тоді канал передання інформації діятиме і надалі [9, *97*].

Інформаційний простір складає інформація відкрита (офіційна), закрита (є державною та комерційною таємницею) та слухова (неофіційна, усна). Використання усіх видів інформації з метою зменшення комерційних ризиків зумовлюється діючим законодавством, практикою, що склалася, та особливостями тієї чи іншої форми діяльності підприємства.

Сама ж система безпеки підприємства може бути комплексна (людина і техніка охорони) та інтегрована (всі наявні підрозділи: охоронні, юридичні, аналітичні, інформаційний, підрозділ технічного захисту інформації та ін.). Йдеться про так звану ділову розвідку. З метою отримання, аналізу, перевірки чи визначення можливостей використання інформації створюється група, що складається з осіб, які:

- здобувають інформацію у підрозділах власної комерційної структури;
- здобувають інформацію з джерел у сторонніх організаціях;
- аналізують, обробляють, накопичують, систематизують інформацію.

Але не тільки ці особи займаються діловою розвідкою. Широка і всебічна система ділової розвідки вимагає участі багатьох підрозділів комерційної установи:

- відділ фінансів. Вивчає матеріали щодо державних і комерційних установ, що відають цінними паперами. Забезпечує постійний фінансовий аналіз конкурентів;
- відділ маркетингу. Забезпечує оцінку ринкових сил, що впливають на поведінку оточення і конкурентів;
- відділ роботи з персоналом (відділ кадрів), проводить співбесіди з тими, хто приймається на роботу і раніше мав справу з конкурентами, підтримує контакти з центрами працевлаштування;
- виробничий відділ. Підтримує контакти з постачальниками обладнання і транспортними організаціями;
- відділ постачання. Відвідує біржі і підприємства, підтримує контакти з постачальниками сировини;
- технічний відділ. Визначає собівартість продукції і слідкує за технічною літературою;
- відділ досліджень. Слідкує за патентами і результатами лабораторних досліджень;
- адміністрація підприємства (установи, фірми). Підтримує контакти з керівниками у своїй галузі (уникаючи розмов щодо цін/видатків), підтримує зв'язки з пресою, асоціаціями, консультантами наукових і промислових сфер.

Таким чином, не можна покладати повну відповідальність за збирання розвідувальних відомостей тільки на керівника служби безпеки. Це навантаження повинно бути розподілене по всьому підприємству, при цьому досягається очевидна перевага: створюється всеохоплююча система, яка значно переважає можливості служби із кількох осіб.

Головне питання полягає в тому, чи є інформація достатньою мірою достовірною і чи дозволяє вона прийняти оптимальне рішення (тобто чи є вона достатньою). Зібрані відомості не є інформацією до того часу, поки вони не проаналізовані і не оцінені кваліфікованими експертами (у невідкладних випадках інформацію можна передавати особам, які приймають рішення, без вивчення експертами, але найбільшу цінність, для тих хто приймає рішення, має опрацьована інформація). Від професійної приналежності аналітика багато в чому залежить і якість оцінки інформації. У

комерційних структурах це означає, що найбільш придатна до цього особа, яка має знання у відповідній функціональній галузі (виробництво, маркетинг, фінанси, дослідження та розробки і т. п.). Аналіз і оцінювання інформації можуть здійснюватися кількома особами, об'єднаними в робочу групу, представниками (фахівцями) різних функціональних підрозділів установи. Але в будь-якому випадку необхідно створювати центр оброблення інформації (для початку для цього достатньо однієї людини). Ця людина підпорядковується керівнику або власнику комерційної структури і, по суті, керує діловою розвідкою.

Незважаючи на те, що система базується на офіційних джерелах, не завжди легко встановити, чи є отримана інформація правдивою, надійною або неправдивою. Можливі два критерії, за якими можна стверджувати про точність інформації: надійність джерела і самої інформації. На сьогодні існує багато методик оцінювання надійності інформації. Одним з найважливіших питань розроблення системи ділової розвідки є її підпорядкованість. Яке місце вона повинна займати в організаційній ієрархії і як вона повинна бути організована? Відповідь на це питання залежить від вимог до цієї системи і, у свою чергу, визначає план діяльності. Якщо вже діє ефективна система маркетингової інформації, служба розвідки може увійти до її складу [1, *301*].

Для забезпечення безпеки використовуються всі наявні на підприємстві сили й засоби. Кожен працівник комерційної структури у межах своєї компетенції повинен брати участь у захисті комерційної інформації, згідно з наявною програмою із забезпечення комерційної інформації.

Також повинна відбуватися координація і взаємодія всередині і поза підприємством. Заходи протидії загрозам здійснюються за координованості усіх підприємств, служб, підрозділів, а також установленні необхідних контактів із зовнішніми організаціями, що здатні сприяти забезпеченню захисту підприємства. Ефективна система захисту дає змогу уникнути прямих і непрямих збитків.

Таким чином, ієрархічна побудова системи безпеки дає змогу стверджувати про її цілісність, так звану взаємодоповнюваність систем: одні системи можуть бути елементами інших систем. Тобто системи складаються із підсистем і входять до складу надсистем. Збільшення ролі недержавних служб безпеки із захисту підприємництва, їх законності та дисципліни є одним з виявів зростаючої соціальної активності громадян України. Правоохоронні органи, спецслужби і суб'єкти недержавної системи безпеки, що діють у сфері захисту законних прав та інтересів підприємців, адміністративно незалежні один від одного, але їх діяльність тісно взаємопов'язана. Схожість напрямів завдань та тісний зв'язок при їх вирішенні створює необхідність взаємодії правоохоронних органів і недержавних структур забезпечення безпеки підприємництва. Безперечно, це зумовлено також тим, що, незважаючи на спільність вирішення завдань із забезпечення безпеки підприємництва, працівники правоохоронних органів та представники недержавних служб безпеки наділені різними повноваженнями. Під взаємодією, у широкому розумінні, мається на увазі узгоджена діяльність адміністративно незалежних один від одного органів і організацій, підприємств щодо виконання спільних завдань. Така форма участі державної системи щодо забезпечення безпеки підприємництва від зовнішніх і внутрішніх загроз об'єднує інтереси органів внутрішніх справ і недержавних структур, що діють у системі безпеки підприємництва. Виходячи з цього державна та недержавна система забезпечення безпеки підприємництва утворюють єдину систему забезпечення безпеки підприємництва України.

Література

1. *Конституція* України. Прийнята на п'ятій сесії Верховної Ради України від 28 червня 1996 р. — К., 1996.
2. *Закон* України "Про захист від недобросовісної конкуренції" від 7 червня 1996 р. // ВВР України. — 1996. — № 24.
3. *Бондаренко Н. И.* Методология системного пордхода к решению проблем. — СПб.: СПГУЭФ, 1997.
4. *Єрмаков І. Б.* Економічна безпека як об'єкт менеджменту // Бізнес і безпека. — 2002. — № 4. — С. 11.
5. *Ильяшенко С. Н.* Составляющие экономической безопасности предприятия и подходы к их оценке // Актуальні проблеми економіки. — 2003. — № 3. — С. 12–19.
6. *Козленко Л.* Информационная безопасность в современных системах управления базами данных // Компьютер Пресс. — 2002. — № 3. — С. 104–108.
7. *Кремер А.* Информационная безопасность как важный элемент управления компанией // Компьютер Пресс. — 2003. — № 9. — С. 55–56.
8. *Медведев А.* Несанкционированное использование информации и способы ее защиты // Отдел Кадров. — 2003. — № 24. — С. 20–24.
9. *Низенко Е. І., Каленяк В. П.* Забезпечення інформаційної безпеки підприємництва. — К.: МАУП, 2006. — 134 с.
10. *Низенко Э. И.* Обеспечение безопасности предпринимательской деятельности. — К.: МАУП, 2003. — 124 с.

11. *Ніколаюк С. І., Никифорчук Д. Й.* Безпека суб'єктів підприємницької діяльності: Курс лекцій. — К.: КНТ, 2005. — 320 с.

12. *Хавронюк М.* Підприємницьке шпигунство і розголошення комерційної таємниці: юридичний аналіз складів злочинів, питання удосконалення відповідальності // Право України. — 1999. — № 9. — С. 45–57.

13. *Чернявский А.* Краткая история развития промышленного шпионажа // Деловая Украина. — 1993. — № 67. — С. 12–18.

14. *Чернявский А.* Методы коммерческой и экономической разведки // Деловая Украина. — 1993. — № 74. — С. 8–15.

З метою забезпечення безпеки підприємницької діяльності на підприємствах, в установах, організаціях за рішенням керівництва створюються служби безпеки. Організація служби безпеки підприємства вимагає ефективного керівництва її роботою. Питання комплексного, системного підходу до забезпечення безпеки підприємництва не є другорядними, тому що вирішуються на базі розроблених фахівцями методик, рекомендацій, що відбивають необхідність практики. Інформаційно-аналітичне забезпечення діяльності щодо захисту підприємництва від зовнішніх та внутрішніх загроз передбачає використання інформації для підвищення рівня виявлення та попередження фактів протиправних дій, підготовки та прийняття відповідних управлінських рішень.

С целью обеспечения безопасности предпринимательской деятельности на предприятиях, в учреждениях или организациях по решению руководства создаются службы безопасности. Организация службы безопасности предприятия требует эффективного руководства ее работой. Вопросы комплексного, системного подхода к обеспечению безопасности предпринимательства не являются второстепенными, а поэтому решаются на базе разработанных специалистами методик, рекомендаций, отражающих потребности практики. Информационно-аналитическое обеспечение деятельности по защите предпринимательства от внешних и внутренних угроз предусматривает использование информации для повышения уровня выявления и предупреждения фактов противоправных действий, подготовки и принятия соответствующих управленческих решений.

For objective of securing safety business activity, making the services of safety in enterprise' or organizations of the resolution leadership, organization service of safety enterprise need efficient leadership her work. The complex of problems, systemic method of approach to ensuring safety business isn't of minor importance. Because, it does decision at basis elaborated specialists' methods, and recommendations what represent necessity practice. Information and analytic securing activity, for safety business of outward and inward influence, menaces foresight taking advantage information's, for unlawful actions preparation, come to decision managerial accordance.

Надійшла 22 січня 2009 р.