ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Л.В. Волчанська, к.е.н., ст. викладач
Дніпровський державний
аграрно-економічний університет

В реаліях сьогочасної української дійсності, що характеризуються високим рівнем нестабільності зовнішнього та внутрішнього середовища, підприємства змушені будувати стратегію власного виживання в ринковому середовищі, засновану на широкому застосуванні інформаційних технологій, одним із основних багатств економічно розвинутих держав. Адже, інформатизація економіки, проникнення її у всі сфери діяльності людини та держави, призвели до того, що економічний потенціал будь-якого суб'єкта все в більшій мірі став визначатися рівнем розвитку інформаційних структур, впливу якого пропорційно зростає й потенційна уразливість економіки.

Інформаційна безпека - найважливіший елемент системи економічної безпеки підприємництва. Заходи із забезпечення інформаційної безпеки, з одного боку, спрямовані на охорону конфіденційної інформації. З іншого - включають контрзаходи, які сприяють розвитку бізнесу і слугують для запобігання неприємним несподіванкам.

Поняття інформації в загальному вигляді містить ст.1 закону України «Про інформацію»: інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інформація на сьогоднішній день є комерційним об'єктом, а отже потребує захисту. Інформаційна безпека заснована не тільки на захисті власної інформації, у тому числі конфіденційної, але й проводить ділову розвідку, інформаційно-аналітичну роботу із зовнішніми й внутрішніми суб'єктами. Інформацію можна продати, купити, імпортувати, фальсифікувати, украсти і т. д. Однак захисту підлягає не будь-яка інформація, а тільки та, котра має ціну, тобто цінна інформація. Цінною ж стає та інформація, володіння якою дасть змогу її дійсному чи потенційному власнику одержати який небудь виграш: моральний, матеріальний, політичний і т. д.

Для захисту інформації в установах спеціально створюється служба безпеки, особливості функціонування якої визначаються тим, що на неї покладені обов'язки з організації режимів конфіденційного діловодства; організації допуску співробітників і сторонніх осіб до конфіденційної інформації; організації зберігання, обліку і знищення носіїв конфіденційної інформації; виявлення каналів можливого витоку інформації, їхня нейтралізація; проведення профілактичної роботи і службових розслідувань; протидії технічним засобам промислового шпигунства; проведення спеціальних акцій, спрямованих на створення сприятливої обставини і нормального функціонування власного підприємства; зв'язку зі службами безпеки інших фірм і державних структур; взаємозв'язку із засобами масової інформації.

Також не менш важливим є захист інформації, яка міститься на машинних носіях. Сюди входить захист конфіденційної інформації, а також захист самих машинних носіїв.

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»).

Для забезпечення інформаційної безпеки підприємницької діяльності необхідна ефективна державна політика, яка передбачає створення загальнодержавної системи інформаційної безпеки. Обов'язковою умовою створення цієї системи є розробка відповідної нормативної бази, розвиток та вдосконалення системи сертифікації систем та засобів захисту інформації, програмних та апаратно-програмних засобів, відтворення системи органів контролю за станом інформаційної безпеки на підприємствах та контроль за їх діяльністю з боку держави; створення сприятливих умов для підприємств, організацій та налагодження виробництва вітчизняних засобів захисту інформації, створення системи підготовки наукових кадрів в галузі захисту інформації; вдосконалення системи підготовки та перепідготовки кадрів для роботи в сфері інформаційної безпеки; врегулювання відносин в галузі використання Internet, створення системи інформаційної безпеки, яка спроможна забезпечити належний рівень її захищеності в умовах постійного удосконалення можливостей технічних розвідок та засобів ведення інформаційних війн, ведення державного контролю за розробкою вітчизняних та ввезення імпортних засобів обчислювальної техніки та ін.

Таким чином, можна зробити висновки, що для створення ефективної системи інформаційної безпеки підприємницької діяльності необхідно:

1. Здійснювати контроль над ймовірними каналами витоку інформації на підприємстві;
2. Здійснювати моніторинг доступу співробітників до корпоративних інформаційних ресурсів;
3. Зберігати архів операцій з документами;
4. Виявляти у вихідному потоці електронної пошти повідомлень, які можуть передбачати загрозу витоку конфіденційної інформації;
5. Виявляти у вихідному потоці даних, які можуть передбачати загрозу витоку конфіденційної інформації;
6. Контролювати використання мобільних пристроїв зберігання інформації, пристроїв передачі інформації і комунікативних портів;
7. Архівувати поштову кореспонденцію;
8. Здійснювати моніторинг на рівні файлових операцій;
9. Контроль за діяльністю співробітників, доступу та використання ними лише тієї інформації, яка потрібна для роботи;
10. Правильний підбір кадрів, застосування матеріальних та моральних стимулів, створення сприятливого соціально-психологічного клімату всередині

організації, створення можливостей для професійного росту, зниження

Однак лише своєчасне та комплексне виконання усіх цих завдань можепризвести до бажаного результату.