Штанько А.В.
студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

ІНТЕЛЕКТУАЛЬНА І КАДРОВА СКЛАДОВІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

На цей час існує дуже багато точок зору щодо визначення суті інформаційної безпеки в бізнесі. Найбільш поширеною із них є думка про інформаційну безпеку як захист інформації з чим не можна погодитись. Оскільки інформаційна діяльність суб'єктів підприємництва пов'язана з мінімізацією інформаційних ризиків, то інформаційна безпека має зачіпати всі складові такої діяльності, а саме інформаційне забезпечення діяльності суб'єктів підприємництва, захист їх інформації та протидію негативному впливу інформаційних технологій, які можуть використовуватись суб'єктами підприємства у їх взаємовідносинах. Виходячи з цього, під інформаційною безпекою суб'єкта підприємництва доцільно розуміти стан, за якого здійснюється ефективне інформаційне забезпечення його діяльності, гарантований захист інформаційного ресурсу та належна протидія негативному інформаційному впливу.

Щодо інформаційних ресурсів підприємства як сукупності інформації слід зазначити, що вони представлені трьома категоріями: документами на паперових і електронних носіях, зразками продукції та інтелектом (знаннями) працівників підприємства [2].

Належний рівень інформаційної безпеки у великій мері залежить від складу кадрів, їх інтелектуального потенціалу й професіоналізму. Незадоволеність персоналу матеріальним становищем або рівнем соціальних гарантій є передзимовою виникнення колізій у інформаційній сфері. Тому постійна увага цьому питанню, роботі з кадрами є одним з головних чинників забезпечення інформаційної безпеки.

Методи охорони інтелектуальної й кадрової складової інформаційної безпеки охоплюють два взаємозалежні й у той же час самостійні напрямки діяльності того або іншого суб'єкта господарювання:

1) орієнтований на роботу з персоналом підприємства (установи), на підвищення ефективності діяльності всіх категорій персоналу;

2) націлений на збереження й розвиток інтелектуального потенціалу, тобто на охорону сукупності прав на інтелектуальну власність (у тому числі на патенти й ліцензії), а також на використання накопичених знань і професійного досвіду працівників підприємства (організації).

Першою стадією процесу забезпечення цієї складової інформаційної безпеки є оцінка загроз негативних впливів і можливих збитків від таких впливів.

Основні негативні впливи на інформаційну безпеку – це недостатня кваліфікація працівників тих або інших структурних підрозділів, їх небажання або нездатність приносити максимальну користь своїй фірмі, готовність за гроші продати відому їм таємницю. Це може бути обумовлене низькою мотивацією персоналу, неефективним керуванням персоналом, відсутністю

коштів на оплату праці окремих категорій персоналу підприємства (організації) або нераціональною їхньою витратою.

Важливою ланкою встановлення нормального рівня інформаційної безпеки є оцінка ефективності заходів, здійснюваних шляхом зіставлення загальної величини витрат на попереджувальні заходи й втрат для підприємства (організації).

Від якості управлінської діяльності у сенсі роботи з кадрами залежать практично усі складові діяльності підприємства, у т.ч. його економічний стан та його інформаційна безпека. При цьому інформаційну безпеку підприємства у розрізі кадрової безпеки слід розглядати у двох аспектах:

- навмисних або випадкових дій персоналу основних функціональних підрозділів, які можуть створювати загрози для підприємства;
- непрофесійних або несумлінних дій співробітників, що забезпечують інформаційну безпеку підприємства, внаслідок чого у системі безпеки можуть виявлятися вразливості.

Таким чином, кадрова безпека повинна створити належні умови для своєчасного виявлення джерела внутрішніх загроз підприємству (зрадник, крадій) та попередження виникнення вразливості у системі безпеки підприємства [4].

Фахівці виділяють кілька критеріїв надійності персоналу, і в ідеалі співробітник комерційного підприємства повинен відповідати кожному з них. До них відносяться:

- професійна надійність;
- психологічна надійність;
- моральна надійність [5].

У сучасних умовах особливої гостроти набуває проблема удосконалення роботи з кадрами, підвищення ефективності професійної діяльності персоналу та забезпечення його психологічної надійності.

Психологічна надійність працівника – це сукупність якостей і можливостей індивідуальності працівника, що обумовлює стан стабілізації його психіки, функціональних резервів організму для виконання найбільш оптимальних дій у складних ситуаціях, а також дотримання ним правових та етичних стандартів поведінки в процесі реалізації функціональних обов'язків [3].

Аналіз конкретних випадків загроз безпеці фірми з боку власного персоналу показує, що виникають вони найчастіше «завдяки» наступним причинам:

- низька кваліфікація;
- моральна незадоволеність роботою;
- шкідливі звички та ін.

Взагалі кажучи, мотивація праці та лояльність фірмі завжди обумовлені безліччю переплетених мотивів. Одним важливий високий заробіток, іншим – кар'єра, третім – соціальна захищеність, четвертим – престиж або можливість займатися творчою роботою. Скривджений співробітник – це міна сповільненої дії, яка рано чи пізно спрацює. Універсальних рецептів, що дозволяють повністю убезпечити фірму від негативних дій власних співробітників, поки ще немає, як немає і засобів забезпечення стовідсоткової безпеки. Однак є можливість максимально знизити цю небезпеку, тримати її під контролем і уникнути небажаних наслідків [5].

Належний рівень інформаційної безпеки значною мірою залежить від інтелекту і професіоналізму кадрів, що працюють на підприємстві. Негативно впливають на цю складову:

- звільнення провідних висококваліфікованих працівників, що призводить до ослаблення інтелектуального потенціалу;
- зниження частки інженерно-технічних працівників і науковців у загальній чисельності працівників;
- зниження винахідницької активності;
- зниження освітнього рівня працівників.

Дії із забезпечення інформаційної безпеки повинні бути регулярним процесом, що здійснюється на всіх напрямках діяльності підприємства, на основі комплексного застосування всіх заходів і засобів безпеки. При цьому засоби та методи безпеки найбільш раціональним способом об'єднуються в єдиний цілісний механізм не тільки для захисту від зловмисників, але і від некомпетентних, недобросовісних працівників та різних непередбачуваних ситуацій. Тобто забезпечення інформаційної безпеки, як і кожної із її складових, має носити системний та комплексний характер [1].

Список використаних джерел:

1. Зубок М.І. Інформаційна безпека підприємства, банку / М.І. Зубок // Бизнес и безопасность. –2011. – № 3. – С. 67-69.
2. Зубок М.І. Інформаційна безпека підприємства, банку / М.І. Зубок // Бизнес и безопасность. – 2011. – № 2. – С. 34-37.
3. Саенко И.Я. Надёжность кадров – коммерческая безопасность предприятия / И.Я. Саенко // Бизнес и безопасность. – 2004. – № 3. – С. 7.
4. Методологія захисту інформації. Конспект лекцій. – Київ, 2011.
5. Ярочкин В.И., Бузанова Я.В. Основы безопасности бизнеса и предпринимательства: Учеб. пособие. – М.: Академический Проект: Фонд «Мир», 2005. – 208 с.

Яковлєв Р.М.
аспірант,
Міжрегіональна академія управління персоналом

РЕФОРМУВАННЯ ОРГАНІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ В УКРАЇНІ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ

Необхідність реформування правоохоронних органів в цілому та органів досудового розслідування, зокрема є беззаперечним фактом і нагальною необхідністю. У спадок від радянського режиму Україні залишилась правоохоронна система, яка, незважаючи на чисельні реорганізації і перетворення, у своїй суті фактично залишається незмінною. Одним із підтверджень цього є місце і роль органів досудового розслідування в зазначеній системі, оскільки, незважаючи на зміни, внесені в кримінальний процес у 2012 році, функції слідчого під час досудового розслідування залишаються зведеними до процесуального оформлення здобутих (як правило внаслідок проведення оперативно-розшукових заходів) доказів.