

ПСИХОЛОГІЧНІ АСПЕКТИ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

А. В. Дудатьєв, к.т.н., доцент

В. М. Дудатьєва, асистент

О. Д. Кец, студент

Вінницький національний технічний університет

dima.kec@gmail.com

Захист інформації розуміє під собою не лише використання відомих механізмів захисту але і кваліфіковані кадри. Відомий факт, що самою слабкою ланкою в цьому ланцюгу є людський фактор. Практично всі підприємства, заводи, корпорації вкладають великі кошти в апаратні засоби захисту інформації, в аналіз, моніторинг, розробку внутрішньої політики безпеки. І в останню чергу звертають увагу на психологічну підготовку спеціалістів, що в більшості випадків призводить до краху всієї системи захисту.

Психологічний вплив може бути як мінімум з двох сторін. В першу чергу із сторони компанії, а саме запровадження контролю щодо стимулювання виконання правил безпеки і певні міри покарання. З іншого боку, це зовнішній вплив на працівника сторонньої компанії. Для цього можуть використовуватися різні методи психологічної атаки, а саме: можливість заробити вкравши інформацію, можливість дезінформування співробітника з метою дізнатися секретну інформацію видаючи її як загальнодоступну. В доповіді розглянуті та запропоновані конкретні рекомендації та механізми щодо використання психологічних аспектів підготовки фахівців у галузі інформаційної безпеки.

У цілому, психологічне забезпечення комерційної таємниці в процесі відбору, підготовки, висування й звільнення кадрів ефективніше й дешевше, ніж при звичайному засекречуванні інформації.

Супровід персоналу є одним з невід'ємних елементів процесу забезпечення корпоративної безпеки кожної фірми й організації.

Моніторинг співробітників необхідний для відстеження змін, що відбуваються зі співробітником у процесі роботи на фірмі, у компанії, організації й появи в нього якостей, що породжують загрозу корпоративній безпеці.

У багатьох компаніях серйозна увага приділяється питанням корпоративного навчання. Таке навчання сприяє виробленню згуртованості, підвищенню працездатності команди, допомагає сформувати резерв на висування.

Поряд з обговоренням професійних питань, у ході навчання повинні розглядатися різні аспекти особистої й корпоративної безпеки.

Основними напрямками навчання можуть стати:

- правила роботи з документами, що містять комерційну таємницю;
- прийоми й методи, використовувані в промисловому шпигунстві;
- ефективна ділова комунікація;
- дії в екстремальних ситуаціях;
- тактика ведення переговорів і протидія маніпулятивному впливу;
- питання особистої безпеки при знаходженні за межами фірми.