Топчій В.В., кандидат юридичних наук, прокурор відділу прокуратури Київської області

ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Оцінка вразливості інформації дає можливість виявити характерні особливості і недоліки об'єкта захисту, які можуть полегшити проникнення конкурента в секрети фірми. І для того, щоб забезпечити ефективний захист інтелектуальної власності необхідно здійснити її аналіз. Його метою є:

- по-перше, визначити вид і потенційну цінність інтелектуальної власності;
- по-друге, оцінити її уразливість (стійкість до засобів розвідки або ураження);
- по-третє, прогнозувати можливість загроз.

Важливим фактором для визначення потреби в заходах, спрямованих на захист інформації, слід вважати і її потенційну цінність для конкурента (супротивника). Вона повинна компенсувати ризик, пов'язаний з отриманням інформації будь- яким способом.

Визначення потенційної цінності інформації дає можливість подумати в першу чергу про безпеку [1, с. 21-22]

найбільш важливих секретів, витік яких здатний завдати шкоди, який значно перевищує можливі витрати на їх захист. При цьому важливо встановити:

- яка інформація потребує захисту;
- кого вона може зацікавити;
- які елементи інформації найбільш цінні;
- який термін існування цих секретів;
- у що обійдеться їх захист [2, с. 14].

Разом з тим, підрахувати точно втрати, які власник або фірма можуть понести в результаті знищення або розкрадання інтелектуальної власності, складно. На думку фахівців, неможливо точно визначити ймовірність реалізації конкретної загрози і розмір пов'язаної з нею шкоди. У зарубіжних аналітичних публікаціях пропонується ряд методик оцінки цих величин. Найбільш проста з них полягає у встановленні кожній загрозі деякої ймовірності «Р», яка визначається виходячи з досвіду експлуатації та наявних статистичних даних. Аналогічним чином оцінюється і величина можливої шкоди «У», що наноситься при реалізації кожної із загроз. Сума утворення цих величин за всіма можливими загрозами дає можливість встановити можливі втрати, а тим самим і розмір коштів, які доцільно затратити на захист.

Якщо в результаті аналізу приходимо до висновку, що та чи інша інформація потребує захисту (постійно або тимчасово) слід приступити до розробки програми її проведення [3, с. 16]. При цьому переслідуються дві мети:

1) запобігання або значне ускладнення розкрадань секретів;

2) доведення до відома всіх співробітників фірми інформації про важливість секретів і заходи покарання за їх розголошення.

Зарубіжний досвід у сфері захисту інтелектуальної власності та вітчизняний досвід в захисті державних секретів показують, що ефективною може бути лише комплексна система захисту, яка поєднує такі заходи:

- використання законодавчих актів, які регулюють питання захисту інтелектуальної власності;
- виконання правил поведінки в колективі, порушення яких веде до втрати авторитету;

- створення перешкод для доступу до охоронюваного обладнання та інформації;

- організація відповідного режиму секретності,
пропускного і внутрішнього режиму і т. п .;

- застосування електронних та інших пристроїв для захисту інформації;

- шифровка інформації;

- застосування спеціальних програм для захисту інформації.

Витік інформації охоплює широке коло різних дій. Це і втрата інформації з комп'ютера в результаті відключення електроенергії, і пропажа документів в результаті їх розкрадання. Втратою вважається і таємне копіювання інформації конфіденційного характеру з одного пристрою, що запам'ятовує, на інший «чужаком», і зняття своїм співробітником «особисто для себе» копії документа, що містить комерційну таємницю.

Витік інформації за своєю суттю та змістом завжди передбачає протиправне (таємне або явне) заволодіння інформацією (виробами, приладами), де міститься комерційна таємниця для того, щоб в корисливих чи інших цілях передати її конкуренту (або іншим зацікавленим особам) [4, с. 54].

Підприємцю важливо мати на увазі два моменти:

1) по-перше, в конкурентній боротьбі треба діяти так, щоб не порушувати закони в спробі заволодіти таємницями конкурента;

2) по-друге, у витоку конфіденційної інформації замішані конкретні особи і часто це співробітники, які працюють в тій чи іншій фірмі, виробництві, цеху.

Не виключається дотримання запобіжних заходів і з боку особи, яка працює на організовану злочинність. Інформація від неї може йти анонімно через підставних осіб, які не мають відношення до злочинної діяльності (в практиці були випадки залучення для цих цілей навіть підлітків), по телефону, телеграфу, поштою і т.д.

Особливе та й, напевно найуразливіше для обох сторін місце займає використання схованок для обміну інформацією, матеріальними предметами, наприклад грошима за роботу.

Організація і зв'язок через тайник вимагає прояву особливого мистецтва і винахідливості. До організації схованки

входить: підбір місця, виготовлення сховища для вкладення переданих речей, розробка операції по використанню схованки.

Місце має бути доступним для обох сторін. Залежно від тривалості зберігання вмісту тайник може бути спеціально обладнаний і камуфльований.

В операцію по використанню схованки входить: розміщення секретних матеріалів в тайник; повідомлення про це адресата; витягнення адресатом вкладення і повідомлення про це першій стороні.

Розмір матеріальної винагороди за надання послуги залежить від змісту інформації, труднощів її добування і т.п. Гроші можуть передаватися поштою чи іншим способом (у залежності від ситуації).

Багато дій, пов'язаних з підготовкою, проведенням і завершенням злочинних посягань, з міркувань скритності проводяться, як правило, на так званих конспіративних квартирах.

Шляхи збору інформації можуть бути найрізноманітнішими. Головне тут - безперервність і постійний аналіз її службової безпеки [5, с. 3].

Таким чином, активна співпраця з комерційними службовцями промислової контррозвідки для приватних фірм необхідна вже зараз і в майбутньому стане неминучою.

Список використаних джерел:

1. Адигюзелов К. А. (Киясудин Ахмедович) Проблемы виктимизации населения (По материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. Махачкала, - 2002. - 199 с.

2. Плешаков В. А. Понятие и виды угроз криминологической безопасности. *Криминологический журнал.* 2006. - № 10. - С. 14-18.

3. Дискуссия по поводу двухуровневого построения системы охраны общественного порядка в Великобритании. Борьба с преступностью за рубежом. 1995. - № 5. - С. 14-17.

4. Сатерленд Э. Х. Являются ли преступления людей в белых воротничках преступлениями? *Социология преступности. Современные буржуазные теории:* сб. статей = The sociology of crime and delinquency: Перевод с англ. / под ред.: Никифоров Б. С. М.: Прогресс, - 1966. - 368 с.

5. Евланова О. А. Участие частных детективных и охранных предприятий в борьбе с преступностью: криминологический

6. аспект: автореф. дис. на соискание ученой степени канд. юрид. наук: 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» М., - 1999. - 24 с.