Виштикалюк М.П.
студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

МЕТОДИ ПРОМИСЛОВОГО ШПИГУНСТВА В СУЧАСНИХ УМОВАХ ТЕХНОЛОГІЧНОГО РОЗВИТКУ

На сучасному етапі інформаційного розвитку та загострення конкурентної боротьби захист власної інформації, «ноу-хау» та науково-технічних розробок набуває першочергового значення. Сьогодні інформація використовується не тільки для задоволення потреб сучасного суспільства, а й забезпечує стабільний його розвиток у всіх сферах діяльності. За цих умов випливає, що інформаційна безпека є найголовнішою складовою діяльності всіх організацій, установ, країн.

Розвиток сучасних інформаційних технологій в економіці, управлінні, банківській сфері сприяв поширенню злочинів у сфері інформаційних технологій, а саме витоків конфіденційної інформації суб'єктів господарювання, яка віднесена до комерційної таємниці. Ці злочини характеризуються складністю фіксації та труднощами з'ясування місця скоєння злочину, широким спектром засобів кодування інформації, слабкими зв'язками між окремими доказами та швидкості знищення даних доказів. Промислове шпигунство є основним способом незаконного отримання інформації, що представляє цінність і може бути комерційною таємницею.

Шпигунство може бути економічне, промислове, комерційне, науково-технічне, але всі вона спрямовані на збір, розкрадання, накопичення і обробку цінної інформації, закритої для доступу сторонніх осіб. Існує чимало методів для збору розвідданих, багато з них не є законними, але всі вони ефективні. Всю сукупність методів які використовуються в промисловому шпигунстві можна розділити на дві групи:

- Агентурні методи.
- Технічні методи.

Основою будь-якого виду шпигунства є агентурний метод отримання інформації. В ньому можна застосовувати два напрямки діяльності: вербування, або впровадження своєї людини. Кожен з них має свої переваги. У будь-якій комерційній структурі є особи, які за своїми знаннями й досвідом наближаються до рівня вищої ланки і які здатні суттєво впливати на хід справ компанії. Вербування може призвести до того, що вигідні угоди та замовлення підуть тим особам, які й організували бізнес-шпигунство. Інколи промислове шпигунства спрямоване знищення фірми-конкурента, тоді впровадження має істотні переваги, тому що довіра до своєї людини, звичайно ж більша, а значить інформацію можна довідатись ціннішу. Об'єктами агентурної розробки не завжди є співробітники які інформовані в справи компанії та плани її розвитку, будь-який працівник зможе здійснити приховане встановлення спеціальних технічних засобів для отримання інформації з обмеженим доступом [1]. Для цього необхідно від декількох секунд до двох-трьох хвилин. А щоби встановити обладнання для перехоплення телефонних повідомлень, взагалі не потрібно проникати в офіс, варто лише знайти телефоніста, який погодиться

знайти потрібний телефонний кабель. Такі «закладки» можуть бути встановлені по лінії телефонного кабелю на відстані до трьох кілометрів від офісу, що значно ускладнює їх виявлення [2].

Щодо технічних методів промислового шпигунства, то необхідно зауважити, що виробництво й збут спеціальних технічних засобів законодавчо врегульовано. А їх несанкціоноване використання карається законом. Для перехоплення і запису акустичної інформації існує велике різноманіття технічних пристроїв: мікрофони, електронні стетоскопи, радіо-мікрофони, лазерні мікрофони.

Непомітне підкидання радіо-передавальних пристроїв – досить поширений спосіб добування інформації. Вони дадуть змогу протягом декількох годин або декількох днів, прослуховувати озвучену в приміщенні інформацію. Час роботи таких «жучків» обмежується лише енергоємністю батареї, але якщо цей пристрій підключити постійного живлення то ним можна користуватися до тих доки його не знайдуть.

Не менш важливими елементами промислового шпигунства є інсайдери та їх інформація. Інсайдерами називають людей які працювали, або працюють з конкурентним підприємством чи організацією і володіють конфіденційною інформацією цього конкурента. Такі люди можуть запросто продати відому їм інформацію.

Основна проблема захисту інформації підприємства зводиться до необхідності і вміння керівників та робітників зберігати і захищати свою інформаційну власність (інсайдерську інформацію). Заходи щодо захисту інтересів підприємства вимагають певних витрат. Існує світова статистика усереднених оцінок. За даними «The Boston Globe», компанії, що входять в число «500 самих щасливих», витрачають сотні тисяч доларів, щоб протистояти електронному шпигунству [3]. Захист кожного об’єкта має бути індивідуальним та комплексним. Для створення ефективного комплексного захисту інформації на підприємстві повинні бути вирішені наступні основні питання:

1. Виявлення інформаційних ресурсів, що підлягають захисту і виділення їх з решти інформації.

2. Оцінка можливого збитку від витоку будь-яких конфіденційних даних і класифікація інформації за ступенем важливості.

3. Визначення усіх видів носіїв інформації, які підлягають захисту.

4. Виявлення можливих факторів вразливості інформації, що підлягають захисту [3].

Отже, із зазначеного можна дійти висновку, що:

1. Промислове шпигунство розвивалося разом з цивілізацією і в момент сучасного технологічного розвитку особливо гострою стає проблема захисту конфіденційної інформації, втративши важливі дані – можна втратити все.

2. Сьогодні існує чимало методів і способів ведення промислового шпигунства. Надійного захисту від них, нажаль, немає. Держава всіляко намагається врегулювати ці питання, але сучасні темпи розвитку технологій неможливо наздогнати.

3. Методи промислового шпигунства можна розділити на технічні та агентурні. Кожен з них має свої плюси і мінуси, але всі вони ефективні при

правильному застосуванні. Щоб їм протистояти потрібно створити і налагодити комплексну, багаторівневу систему захисту.

Список використаних джерел:

1. Ткачук Т.Ю. Характерні особливості конкурентної розвідки та промислового шпигунства // [Електронний ресурс]- Режим доступу http://personal.in.ua/article.php?ida=451
2. Березин І. Промислове шпигунство, конкурентна розвідка, бенчмаркинг й етика цивілізованого бізнесу // Практичний Маркетинг. – 2005. – 22 липня. – № 101.
3. Вовченко В.В. Проблемы защиты информации от экономического шпионажа / В.В. Вовченко, И.О. Степанов // [Електронний ресурс]- Режим доступу http://www.analitika.info
4. Теорія економічного аналізу: Навч. посіб. / Купалова Г.І. – К., 2008. – 639 с.

Задушинський О.П.
студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

СУБ'ЄКТИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ: ПОНЯТТЯ ТА ВИДИ

Важливим аспектом розвитку суспільства є інформаційно-комунікативна діяльність, яка в сучасних умовах визначально впливає на формування інформаційної політики. Політика завжди пов'язана з потребами та інтересами людей, з реалізацією владних функцій, з діяльністю інститутів громадянського суспільства і держави; вона знаходить відображення і вираження в суспільній, масовій свідомості, громадських настроях, соціальному самопочутті.

Тотальна глобалізація та інформатизація усіх сфер життєдіяльності людської цивілізації гостро визначає проблему інформаційної політики України, яка стає все більш нагальною.

Захист інформаційної безпеки здійснюється шляхом проведення виваженої та збалансованої політики держави в інформаційній сфері. Враховуючи, що політика інформаційної безпеки як суспільне явище має комплексний характер і включає внутрішньо і зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому вона потребує комплексного підходу через призму норм адміністративного права у формуванні, адже йдеться саме про проведення державної політики, тобто певних владних відносинах. Сьогодні інформаційна сфера є інтегруючою основою життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних основ його подальшого розвитку. При таких умовах особливого значення набуває формування виваженої державної інформаційної політики на основі системних наукових досліджень явищ інформаційної сфери, провідне місце серед яких займає інформаційна безпека.

Інформаційний простір завдяки трансграничності та віртуальному характеру виступає в сучасному світі як одна з основних сфер інтеграції людського співтовариства в планетарних масштабах [4].